

# **Teague**

## **Police Department**

### **Policy Manual**



Issue Date: November 15, 2021

## TABLE OF CONTENTS

Chapter and Topic	Policy #
<b>Chapter 1 Administration and Organization</b>	
Chief's Message	1.0
Mission, Values, Written Directives	1.1
Law Enforcement Role and Authority	1.2
Fiscal Management	1.3
Inspections and Audits	1.4
Mutual Aid Agreements	1.5
Departmental Reports	1.6
Goals and Objectives	1.7
<b>Chapter 2 Professional Standards and Conduct</b>	
Rules of Conduct	2.0
Bias Based Policing	2.1
Sexual Harassment or Other Illegal Harassment	2.2
Internal Investigation Process	2.3
Employee Disciplinary Process	2.4
Accident and Injury Prevention	2.5
Court Appearance	2.6
Use of Social Media	2.7
<b>Chapter 3 Training</b>	
Basic Training Requirements	3.0
Field Training	3.1
<b>Chapter 4 Personnel</b>	
Hiring and Selection	4.0
Appointment and Probation	4.1
Career Development, Promotions, and Transfers	4.2
Performance Evaluations	4.3
Uniforms, Appearance and Equipment	4.4
Outside Employment	4.5
Grievance Procedure	4.6
Reserve Officer Program	4.7
Community Outreach and Customer Service	4.8
<b>Chapter 5 Departmental Records</b>	
Departmental Records	5.0
Media and Public Information	5.1
Computer and Electronic Equipment Usage and Data Security	5.2
<b>Chapter 6 Use of Force</b>	
Use of Force	6.0
Firearms and Qualification	6.1
Less-than-Lethal Weapons	6.2
Officer Involved Shooting Investigations	6.3
Chaplaincy Program	6.4
Support of Officers Involved in Critical Incidents	6.5
Mental Health Wellness Checkups	6.6
Mental Health Leave	6.7

## **Chapter 7 Law Enforcement Operations**

### **Legal Issues**

Constitutional Safeguards	7.0
Field Interview, Consensual Encounters and Detentions	7.1
Arrests With and Without A Warrant	7.2
Search Incident to Arrest and Other Searches Without a Warrant	7.3
Search Warrants	7.4
Limited English Proficiency	7.5
Communication with the Deaf or Hard of Hearing	7.6
Arrests of Transgender, Intersex, Gender Nonconforming (TIGN) Individuals	7.7
Citizens or Media Recording of Police Activity	7.8

### **Field Operations Issues**

Prisoner Restraints	7.10
Prisoner Transportation	7.11
Juvenile Procedures	7.12
Domestic Violence and Protective Orders	7.13
Vehicle Operation	7.14
Vehicle Pursuits	7.15
Vehicle Impoundment and Inventory	7.16
Communicable Diseases	7.17

### **Patrol Operations**

Patrol Operations	7.20
-------------------	------

### **Traffic Operations**

Traffic Enforcement	7.30
Accident Investigation	7.31

### **Investigative Operations**

Investigations	7.40
Crime Scene Processing	7.41
Eyewitness Identifications	7.42
Informants	7.43
Sex Offender Registration	7.44

## **Chapter 8 Unusual Occurrences**

Unusual Occurrences and Special Events	8.0
Civil Disturbances and Mass Arrests	8.1
Assisting Mentally Ill	8.2
Assisting Developmentally Disabled	8.3
Active Shooter Response	8.4

## **Chapter 9 Prisoner Processing and Custody**

Prisoner Processing	9.0
---------------------	-----

## **Chapter 10 Court Operations**

Municipal Court Operations	10.0
----------------------------	------

## **Chapter 11 Property and Evidence**


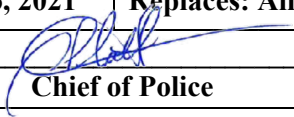
Property and Evidence Management	11.0
----------------------------------	------

**Appendices and Forms**

Appendix A  
Employee Leave Request 2.2018  
Equipment Issue Form  
Family Violence Worksheet  
Field Identificaiton Form  
Informant Agreement  
Notification of Emergency Detention - CIT Form  
Notification of Student Arrest  
Off Duty Employment Request  
Officer Evaluation Form  
Overtime Notification  
Performance Improvement Plan - 30 day Evaluations  
Personal History Statement 08-12-2020  
Photo Line Up Form  
PIR - Records and Accident Request  
Property - Evidence Room Inspection Report  
Receipt for Child  
Receipt for Criminal Cases  
Receipt for Property  
Receipt for Warrants  
Request for Prosecution  
Teague PD Strangulation Supplement  
Teague Police Job Descriptions  
Teague Police Officer Complaint Form  
Use of Force Form  
Vehicle Monthly Check Sheet  
Vehicle Pursuit Report Form  
Voided Citation Memo  
Voluntary Statement of Accused  
Voluntary Statement of Accused Continued  
Voluntary Statement - Not Arrested  
Voluntary Statement Continued - Not Arrested

**Manuals**

Background Investigation Manual  
CJIS Security Policy V. 5.9  
Field Training Manual  
FTO Recruit Training Guide  
Patrol SOP  
Performance Evaluation Manual  
Report Writing Manual

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 1.0 Chief's Message</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
	<b>Reference:</b>	


I am proud to present the newest edition of the Teague Police Department Policy Manual; all previous versions of the Teague Police Department Policy Manuals are hereby rescinded and no longer utilized as a guiding principles for this department as of November 15, 2021.


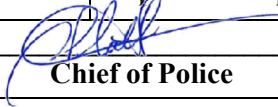
The policy manual is the foundation for all the department's operations and, when properly implemented, provides staff with the information to act decisively, consistently, and legally. It also promotes confidence and professional conduct among staff members. Adherence to these policies helps safeguard employees and the department against civil litigation, ensuring employees will be protected when their individual actions are scrutinized, especially after a critical incident.

Department employees should understand that policy consists of principles and values which guide the performance of departmental activity. Policy is not a statement of what must be done in varying situations. It is a statement of guiding principles which should be followed in activities which are directed toward the attainment of departmental objectives.

All employees shall abide by these policies and are responsible for keeping themselves current on the content of this manual and any updated policies that may come later.

I want to thank all departmental staff members for their commitment to excellence and service to our community.

  
 D. DeWayne Philpott  
 Chief of Police

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 1.1 Mission, Values, and Written Directive System</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All previous versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 1.04</b>	

## I. POLICY

Law enforcement agencies provide essential services to foster safe communities through crime reduction and deterrence. Administrators of these law enforcement agencies are obligated to train, supervise, and guide personnel in performing the myriad tasks that are necessary for creating safe communities.

At the same time, these administrators must seek to improve employee confidence and competence in performing tasks while reducing vulnerability to liability. To meet these obligations, agencies must manage themselves according to written directives. A manual of policies and procedures guides the day-to-day legal and ethical functioning of a law enforcement agency.

To that end, this manual furnishes a blueprint for the performance of this agency’s activities in accordance with established state and national standards. Providing all members of the department with an understanding of the department’s mission and its values provides guidance for decision making when situations are not covered by direct policy or procedure.

## II. PURPOSE

This document outlines the organization of the department, its *Policy and Procedure Manual*, and its authority. It also defines three kinds of statements that appear in these documents -- policy, rules, and procedures -- and states the department’s mission and core values.

## III. AGENCY MISSION AND VALUES

### A. Mission:

It is the mission of the Teague Police Department to provide the highest levels of proactive and responsive service to the City of Teague in partnership with neighborhoods and the community. We shall endeavor to detect and solve problems that will afford the citizens of Teague with the highest quality of life possible. This service shall be provided with integrity, equity, and excellence.

## B. Core Values

Dedication to the Department's mission and professional conduct in providing caring services is essential to community support and successful performance.

Positive contributions and innovation are supported and encouraged in achievement of departmental goals.

Pride and integrity are the direct result of individual honesty, interpersonal trust, teamwork, and open communications at all levels.

Authority must be willing to accept personal responsibility and accountability for their decisions.

Our future is determined by the development and maturity of each individual member and we subscribe to the following values:

**INTEGRITY** -- I will always maintain my personal integrity in all that I do, at work and at home.

**EXCELLENCE** -- I will always pursue excellence for myself and the Teague Police Department.

**FAIRNESS** -- I will always treat all people fairly.

**PRIDE** -- I will take pride in myself, my department and my profession and shall always maintain their honor.

**HONESTY** -- I will always be honest; honest to myself, to my supervisors, and to the public.

**SERVICE** -- I will always endeavor to provide the highest level of service.

**COMPASSION** -- I will always be compassionate.

**INNOVATION** -- I will always endeavor to be innovative, looking for new and better ways to do things.

## IV. DEFINITIONS

A. Policy: A policy is a statement of the department's philosophy on a given issue.

1. Policy consists of principles and values that guide the performance of department employees.
2. Further, policy is based upon ethics, experience, the law, and the needs of the community.

3. Each section of the manual will begin with an agency policy statement.
4. Only the Chief of Police determines policy.

B. Rule: A rule is a specific prohibition or requirement governing the behavior of employees.

1. Rules permit little, if any, deviation. The violation of a rule normally results in discipline.
2. Rules appear in the *Policy and Procedure Manual* as well as other departmental documents.

C. Procedure: A procedure defines the acceptable method of performing an operation or activity. It differs from policy in that it directs employees' actions in performing specific tasks in a prescribed manner within the guidelines of policy.

1. Failure to follow a procedure may or may not result in disciplinary action, depending on the circumstances.
2. Procedures constitute the agency-approved guide to performing tasks.
3. Employees may depart from procedures only when, in their professional judgment, the situation warrants.
4. Employees must be prepared to justify their actions if they decide not to follow the defined procedure.

D. Memorandum: A memorandum provides useful, specific information to employees and may constitute a directive affecting specific behavior for a specific event or timeframe and is usually self-canceling.

NOTE: Memoranda are not part of this manual; however, memoranda may be incorporated into future editions of the policy manual. Memoranda may be issued by the Chief of Police or by other personnel or agencies. Employees are advised that they may not alter components of this manual based on memoranda unless the memo was issued by the Chief of Police or a designee.

## V. WRITTEN DIRECTIVES (Texas Best Practices 1.04)

A. Departmental Policy Manual and Standard Operating Procedures.

1. The policy manual contains policy statements, rules, and procedures as defined above, and is a written directive governing organizational matters.
2. A standard operating procedure (SOP) primarily contains procedures, and is a written directive governing operational matters and routine daily tasks, such as how to respond to alarms, how to book a prisoner, etc.




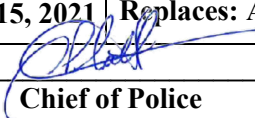
- a. Because they contain many procedural statements, SOPs permit some discretion. While SOPs are the preferred method of accomplishing a task, the agency recognizes that an employee may depart from procedures, if unusual circumstances warrant, and supervisors approve. Employees must justify their actions and document any departure from a standard operating procedure.
  - b. The Chief of Police approves all SOPs.
- B. No policy, rule, regulation, procedure, or memorandum is valid unless signed by the Chief of Police.
- C. Within the context of any directive, the use of the word "shall" or "will" denotes an action or behavior that is mandatory and unequivocal. The words "may," "can," or "should" denote an action or behavior that is discretionary.
- D. Any member of the department may suggest or recommend changes to the Chief of Police concerning the *Policy Manual* or an SOP by forwarding the suggestion through the chain of command.
- E. The Chief of Police or a designee will completely review the policy manual and the standard operating procedures at least biennially to ensure continued compliance with Texas law and operations. Revisions may be made at any time. Once a revision is approved and published, each employee shall be deemed to be on notice with regards to the current version.

NOTE: The office of the Chief of Police is responsible for distribution of all material to the employees of the department. A system for ascertaining that each employee has received the material must be set up and maintained. It must include a method for determining that each employee has received the information.

## **VI. COMPLIANCE WITH DIRECTIVES**

- A. All employees of this department shall read, adhere to, and are held accountable for all directives, policies, procedures, rules, and instructional training material that they have received and signed for.
- B. All employees are responsible for adherence to all written directives that they have signed for and that affect the employee and the employee's work status.
- C. All employees are responsible for maintenance of all directives that are distributed to that employee. Each employee of the department shall sign a statement acknowledging that the member has received, read, understands, and agrees to abide by the directive supplied to them in the appropriate manual(s), including revisions. If an employee does not understand the content of an order or directive or believes that an order or directive is illegal or in conflict with other orders or directives, he or she should immediately notify a supervisor who shall provide instruction or training as necessary.

- D. Copies of the statements of receipt (see above) shall be maintained in the written directive file.
- E. All employees shall comply with the provisions of these directives and with the City Employee Handbook. If an issue is not addressed in the Employee Handbook, these directives shall apply. In the event a conflict exists between these directives and the Employee Handbook, the Employee Handbook shall control unless the Department Policy Manual is more restrictive.
- F. The policies in this manual and the standard operating procedures (SOPs) apply to all sworn officers and non-sworn employees of the police department both on and off duty.

	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 1.2 Jurisdiction, Organization, and Authority</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____ <div style="text-align: center;">   <b>Chief of Police</b> </div>
	<b>Reference:</b> Texas Best Practices 1.01, 1.05, 1.06, 1.07, 2.03, 3.07, 6.05, and 8.10.

## I. POLICY

The police department is established by state law and local ordinance. It is comprised of a Chief of Police and other full-time and reserve officers, along with non-sworn employees as determined by the Board of Aldermen through needs of city services. The Chief executive of the police department is the Chief of Police, appointed by the Board of Aldermen. The Chief appoints police officers who are charged with enforcing the laws of the State of Texas and all local ordinances. The jurisdiction of the police department is limited to the city limits, except in cases of pursuit of offenders who have committed a violation within the city limits and flee outside the city limits, when another agency requests assistance, when enforcing laws on property owned by the city but outside its incorporated boundaries, and as authorized by Texas statutes. The organization of the police department shall support the effective and efficient accomplishment of departmental responsibilities and functions according to community-oriented policing principles.

## I. PURPOSE

The purpose of this policy is to describe the jurisdiction and organization of the police department, outline its rank structure, and assign responsibilities, functions, and duties.

## II. AUTHORITY AND AGENCY JURISDICTION

The jurisdiction of the Teague Police Department is limited to inside the city limits of the city with certain exceptions as noted in Texas statutes. (Texas Best Practices: 1.05, 1.06)

- A. Police officers appointed by the city have all the authority granted to them by the State of Texas as Peace Officers. Appointed officers have the responsibility to act within the law, preserve order, arrest offenders, and protect the residents and visitors to our city.

- B. Officers have arrest authority anywhere within the State of Texas; however, the exercise of that authority will be limited when outside the city limits to those situations involving a felony or the use of violence or threatened use of violence against a person, and then only to the extent that the officer is able to safely intervene. Enforcement of traffic laws, although allowable under Code of Criminal Procedures, will be limited to situations in which the public is at risk of injury, serious injury, or death. When off-duty or out of our primary jurisdiction, officers seldom have appropriate equipment, communications, or the assistance needed to properly intervene in dangerous situations. Intervention in these cases may be resolved by calling appropriate authorities and remaining on scene to provide witness information. (An official map of the city limits will be maintained in each patrol briefing room.)
- C. Officers have authority to enforce the law on property owned by the city but is situated outside the city limits.
- D. Officers have authority to pursue offenders outside the city limits who have committed violations inside the city pursuant to the department's pursuit policy. When investigating a crime that occurred inside the city, officers may utilize their authority to conduct investigations, including interviewing witnesses, interrogating suspects, executing search and arrest warrants, and making lawful arrests without warrants anywhere in the State of Texas.
- E. Officers have authority to enforce the law in another jurisdiction pursuant to a properly executed mutual aid agreement or as prescribed by Texas statutes.
- F. While officers have full authority to make arrests, issue summonses, and use force in enforcing the law, officers are also expected to use discretion and common sense in the application of this authority. Officers should always seek the least intrusive level of intervention appropriate to preserve the peace and protect the public safety.

### **III. ORGANIZATIONAL STRUCTURE, CHAIN OF COMMAND, AND AUTHORITY**

#### **A. Organizational structure**

1. Texas Local Government Code Section 341 – Type A General Law Municipality: authorizes the establishment and regulation of a municipal police force by a governing body. On February 23, 1970 the City of Teague Board of Aldermen, by majority vote, established the Teague Police Department. The Office of Chief of Police is through appointment by the Board of Aldermen. The Chief of Police is responsible for directing all activities of the department. This direction is accomplished through written and oral orders as well as by personal leadership. Written orders take the form of general orders, standard operating procedures, and other directives as needed.
2. The department consists of a police Chief, two sergeants, and as many police officers as the Board of Aldermen determines are required to protect and serve the community and otherwise support or carry out the department's objectives.

## B. Chain of Command and Succession

1. The Chief of Police has full control over departmental activities. In the absence of the Police Chief, the senior sergeant shall take command and notify the Chief of all major decisions that he or she may make. If the Chief and the senior Sergeant are not available, then the second sergeant or senior patrol officer shall take command until a ranking officer is available and shall make any necessary reports to the Chief.
2. Supervisors shall, without specific instructions, undertake the required details and assignments necessary to carry out the business of the department. Supervisors shall be guided in the assignment of personnel by the number of officers available for duty and the necessity to assign them where they will be most useful.
3. Plans for any event utilizing departmental personnel will clearly delineate the command structure and outline the span of control.

## C. Authority and responsibility

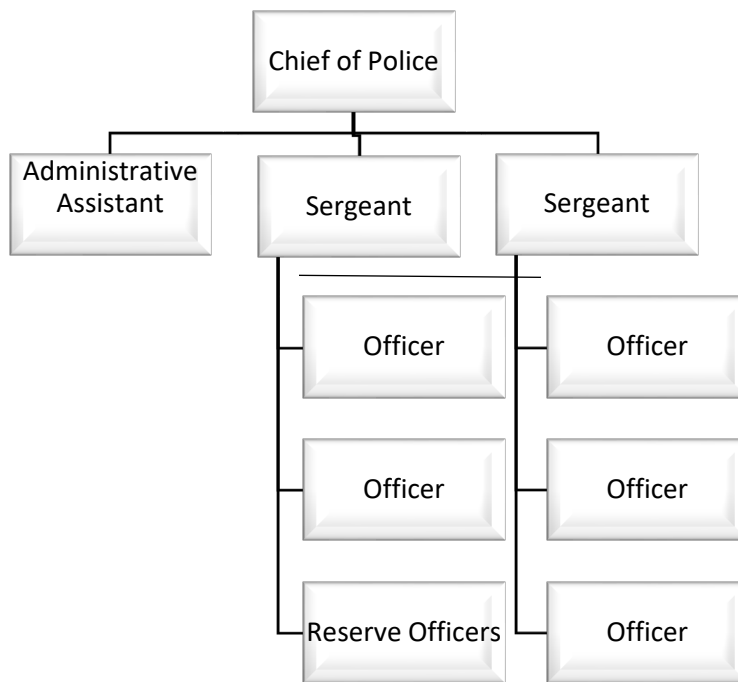
1. At each rank within the department, personnel are given the authority to make necessary decisions for the effective performance of their responsibilities. The department is committed to fostering an organizational climate that rewards employees for initiative, innovation, community involvement, and problem solving.
2. Each employee shall be held accountable for the use of, or failure to use, delegated authority. Any employee with questions concerning his or her delegated authority shall refer the matter to the on-duty supervisor or the Chief of Police for prompt resolution.
3. Supervisors will be held accountable for the condition and preparedness of the personnel assigned to them.
4. Supervisors are responsible for the good order and sanitary condition of department offices, vehicles, and equipment.
5. Supervisors are responsible for the efficiency, discipline, and morale of employees under their charge. Supervisors shall investigate or cause to be investigated all allegations of employee misconduct. Supervisors shall make a report to be forwarded to the Chief of Police detailing the allegations and their findings.
6. Supervisors shall ensure that employees have been supplied with all appropriate written orders and shall instruct them thoroughly on all oral and written orders. Supervisors shall regularly review and instruct subordinates in pertinent laws, ordinances, and necessary skills.

D. Authority of the Chief of the Police Department (Texas Best Practices: 1.07)

1. As the Chief executive of the department, the Chief of Police has full authority and responsibility for the management, direction, discipline, and control of the operation and administration of the department.
2. The Chief of Police shall attend the initial police training provided by the Law Enforcement Management Institute of Texas as required by the Texas Education Code 96.641(h), within 12 months of appointment.
3. The Chief of Police is also the Departmental Homeland Security coordinator and will maintain relationships with the State Homeland Security office and other state and federal Homeland Security resources. (Texas Best Practices: 8.10)

E. ORGANIZATIONAL CHART (Texas Best Practices: 1.01)

1. The attached chart denotes chain of command and intra-department relationships.



2. The organizational chart is reviewed annually and updated as necessary to illustrate the current functioning of the department.

F. OATH OF OFFICE REQUIRED (Texas Best Practices: 2.03)

1. All sworn officers will swear or affirm any oath required by state law or city ordinance before assuming law enforcement duties. All sworn officers shall abide by the Law Enforcement Officer's Code of Ethics. A copy of the law enforcement Code of Ethics is provided to each sworn officer and is further incorporated herein:

## **Law Enforcement Code of Ethics:**

*“As a law enforcement officer, my fundamental duty is to serve mankind; to safeguard lives and property, to protect the innocent against deception, the weak against oppression or intimidation, and the peaceful against violence or disorder; and to respect the Constitutional rights of all persons to liberty, equality and justice.*

*I will keep my private life unsullied as an example to all; maintain courageous calm in the face of danger, scorn, or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed in both my personal and official life, I will be exemplary in obeying the laws of the land and the regulations of my department. Whatever I see or hear of a confidential nature or that is confided to me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.*

*I will never act officiously or permit personal feelings, prejudices, animosities, or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately without fear or favor, malice or ill will, never employing unnecessary force or violence and never accepting gratuities.*

*I recognize the badge of my office as a symbol of public faith, and I accept it as a public trust to be held as long as I am true to the ethics of the police service. I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession...law enforcement.”*

2. Such oath shall be made in public and shall be witnessed by the city secretary or other notary who shall witness and record it on the form approved by the department. The oath shall be filed in the officer’s personnel file.

### **G. AUTHORITY TO CARRY WEAPONS AND USE FORCE (Texas Best Practices: 6.05)**

1. Sworn officers who are licensed peace officers of the State of Texas are authorized to carry firearms and other weapons as identified in these directives, and to use force when necessary and to the extent authorized by these orders and state law in enforcing the law and protecting the public.
2. Sworn officers who are off duty are encouraged to carry firearms to act when necessary to preserve life and property. When not in uniform, officers will not allow any weapon to be visible to the public, except for normal investigative duty assignments.
3. Officers are not to carry any weapon when off-duty if they have consumed or intend to consume any alcoholic beverages, prescription drugs, or other medication, or by a physical ailment or injury.

## H. OFF-DUTY AUTHORITY

1. **Liability Protection:** Officers of this agency have liability protection for the on and off-duty performance of official duties. This protection does not extend to those actions that the police officer knew, or reasonably should have known, conflicted with the law or the established policies of this department.

Authorized Off-Duty Arrests: When off duty an officer may make an arrest only when all the following occur:

- a. There is an immediate need to prevent a crime or apprehend a suspect.
  - b. The crime would require a full custodial arrest.
  - c. The arresting officer possesses appropriate police equipment and police identification.
  - d. The officer complies with Texas Code of Criminal Procedures Article 14.03 (Authority of Peace Officers) and the policies herein.
2. **Off-Duty Responsibilities**

While off duty, the police officer is responsible for immediately reporting any suspected or observed criminal activities to on-duty authorities. When an officer is prohibited from taking off-duty enforcement actions under provisions of this policy, the officer shall act as a trained observer and witness to the offense and shall summon on-duty personnel as soon as reasonably possible. Where an arrest is necessary, the off duty arresting officer shall abide by all departmental policies and procedures.

3. **Prohibitions of Off-Duty Arrests**

Even though a police officer has police powers and responsibilities 24 hours a day throughout the jurisdiction, the off-duty officer generally should not attempt to make arrests or engage in other law enforcement actions when the provisions of this section are not met or when any of the following circumstances exist:


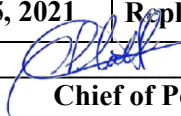
- a. The officer is personally involved in the incident underlying the arrest.
- b. The officer is engaged in off-duty employment of a non-police nature.
- c. The officer's ability or judgment to use a firearm or take a person into custody has been impaired by use of alcohol, prescription drugs, or other medication, or by a physical ailment or injury.
- d. A uniformed police officer is readily available to deal with the incident.



4. Off-duty officers in plain clothes shall follow all orders issued by uniformed officers without question or hesitation during enforcement encounters and shall identify themselves as law enforcement officers as prescribed by departmental training. The department's training authority shall establish protocols (including the use of signs and signals) for recognition of off-duty officers in plain clothes to reduce the potential of misidentification of such personnel during enforcement encounters. Such protocols shall be reviewed periodically during in-service training.

#### I. RESERVE OFFICERS

1. Reserve officers are authorized by the Board of Aldermen, by ordinance. Reserve officers have the same authority and responsibility as regular sworn officers when on-duty and working for the department. They are bound by the same policies and standard operating procedures as regular officers.
2. Reserve officers are required to have the same level of both initial and in-service training as regular officers. (Texas Best Practices: 3.07)
3. Reserve officers who are off duty are encouraged to carry firearms to act when necessary to preserve life and property. When not in uniform, officers will not allow any weapon to be visible to the public, except for normal investigative duty assignments.
4. Reserve Officers are not to carry any weapon when on or off-duty if they have consumed or intend to consume any alcoholic beverages, prescription drugs, or other medication, or by a physical ailment or injury.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 1.3 Fiscal Management</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 1.02, 1.03 and 1.10</b>	

## I. POLICY

It is the policy of the Teague Police Department to maintain the highest level of fiscal responsibility. The Chief of Police is responsible for the development and submission of the departmental budget as well as the financial management of the department. It will be the policy of the department to maintain accurate and detailed records of all monetary transactions to remain above reproach.

## II. PURPOSE

The purpose of this policy is to establish procedures for employees making routine and emergency expenditures for goods or services necessary for the efficient operation of the department.

## III. STATEMENT OF SPECIFIC RESPONSIBILITY

The Chief of Police, as a department head of the City of Teague, Texas, has the authority and responsibility for the fiscal management of the department. (TEXAS BEST PRACTICES: 1.02)

## IV. DEFINITIONS

- A. Routine Expenditure: Purchases that are budgeted and/or planned for and handled through the city purchasing department.
- B. Emergency Expenditure: A use of city funds necessary to accomplish vital goals of the department that by their nature cannot be postponed until regular business hours. These expenditures might be for goods or services. Emergency expenditures are always more than fifty (\$50) dollars and are approved by the Chief of Police.
- C. Purchase Order (P.O.): An authorization from the city purchasing office for payment to a vendor for goods or services.
- D. Purchase Order Number (P.O. #): The number assigned by the city purchasing office for a specific expenditure. Vendors consider a P.O. # the same as cash, and it must be indicated plainly on all invoices.

- E. Vendor: Any authorized retailer, wholesaler, manufacturer, or other supplier of goods or services to the City of Teague.
- F. Tax Exemption Certificate: A document provided to vendors by the city purchasing office that indicates that purchases made for city use are exempt from state sales tax.
- G. Requisition: The form used to request goods or services.
- H. City Purchasing Office: The authority in the City of Teague with the responsibility of exercising fiscal control over all expenditures made by city employees.
- I. Payment Authorization Form: The document used in lieu of a purchase order for the following items: (a) freight bills, (b) travel expenses, (c) authorized organization dues, (d) equipment rentals exceeding two months, (e) advertising, (f) purchases from vendors who do not accept purchase orders and require check or cash.

## **V. RESPONSIBILITIES**

- A. The Chief of Police has the ultimate authority, responsibility, and accountability for the fiscal management of the department.
- B. The Chief of Police prepares the departmental budget with input from supervisors and officers of the department.
- C. Supervisors are responsible for providing budget requests that contain any necessary documentation for their areas during the budget preparation process.
- D. The Chief of Police is also responsible for at least a monthly review of the budget to include the amount budgeted, the amount spent year-to-date by category, and the amount remaining. Any projected budget shortfall shall be discussed with the City Administrator as soon as it is discovered.

## **VI. GENERAL PROCEDURES**

The city purchasing office is responsible for monitoring the suitability of vendors, and the police department will not purchase goods or services from any vendor currently under suspension by the city.

## **VII. COLLECTION AND DISBURSEMENT OF CASH (TEXAS BEST PRACTICES: 1.03)**

- A. All cash funds, financial transactions, or accounts from which department employees are permitted to receive, maintain, or disburse cash (such as petty cash, purchase of reports, licenses, etc.) will include:
  1. A balance sheet or some other system listing initial balance, credits, debits, and balance on hand.
  2. A listing of cash received and from whom it was received.

3. Records, receipts, documentation, and invoices showing expenditures.
- B. All cash funds will be kept under lock and key. The Chief of Police and City Administrator will determine which personnel will have access to the funds and the log or balance sheet. No unauthorized person shall be permitted access to any funds, the log, or balance sheet.
- C. No employee shall accept or disburse cash without prior written authorization of the Chief of Police.
- D. The Chief of Police, or his designee, is responsible for management and security of each cash fund.
- E. Cash funds maintained at the police department shall be kept secured in a locked container (e.g., cash drawer, lock box, etc.)
- F. A quarterly audit will be conducted on each cash account by a person other than the custodian of the account. A different person should conduct the audit each time.
- G. A fund that contains cash received by department units for the use and benefit of employees, such as a fund from candy and soda machine sales, shall be maintained in the same way as any other fund, and records reported to the Chief of Police at quarterly.
- H. A member of the city finance department will audit each account at least quarterly.

## **VIII. EMERGENCY EXPENDITURES**

NOTE: Emergency expenditures over \$1,000 require purchasing department approval.

- A. Any police employee needing to make an emergency expenditure will submit a memorandum through the chain of command that provides the following details:
  1. What the expenditure is for.
  2. Why the expenditure constitutes an emergency.
  3. The cost of the expenditure.
  4. Names of three possible vendors if the expenditure is for more than \$50.
- B. The Chief of Police or designee is responsible for:
  1. Deciding whether the expenditure is an emergency.
  2. Causing the memorandum to be marked "approved" or "disapproved" and initialed.
    - a. If the request is approved, the Chief or designee will cause the bidding of the goods or services requested to be made, awarding the bid to the lowest bidder conforming to specifications and delivery requirements.

- b. If the request is disapproved, the Chief or designee will notify the requesting person to proceed with a routine requisition discussed later in this policy.
- C. It is the responsibility of the employee receiving authorization for an emergency expenditure to:
  1. Plan with the approved vendor to provide the goods or services.
  2. If the vendors request a tax-exempt number, give them the Tax ID Number.
  3. If the vendor asks for a tax exemption certificate, advise them that you will request the police department's fiscal office to forward a tax-exempt certificate to them on the next business day.
- D. It is the responsibility of the Chief of Police or designee to:
  1. Provide to the purchasing department an itemized list of the goods or services obtained, including the total cost.
  2. Obtain a purchase order number and cause it to be added to the report to the purchasing department.
  3. Forward a copy of the report, along with all invoices or receiving slips, including the P.O.#, to the purchasing department.
- E. It is the responsibility of the Chief of Police or designee to prepare a requisition, attaching all invoices or receiving slips, and forward it to the city purchasing office and arrange for out-of-pocket cash reimbursements, where applicable, using a payment authorization form with the receipts attached.

## **IX. ROUTINE EXPENDITURES**

- A. It is the responsibility of any police employee needing to make a routine purchase of goods or services to:
  1. Obtain approval of the Chief of Police, or his designee.
  2. Create an informal memorandum that provides the reason and the type of service or goods to be purchased.
  3. Hand carry the request to the Chief of Police, or his designee.
  4. Contingent on approval, receive a purchase order number from the Chief of police, or his designee.
  5. Arrange for the delivery of goods or services by the vendor.
  6. Return all invoices and/or receiving slips to the fiscal manager on the next business day following the receipt of goods or services.

- B. Prior to approving the request, it is the responsibility of the Chief of Police, or his designee to secure adequate documentation for the purchase and ensure that budgeted funds are available.
- C. Purchases of items costing more than \$1,000 are made after a requisition for material has been approved by the city purchasing office and a purchase order number has been issued in accordance with this policy.
  - 1. The requisition form will be used prior to the purchase except in emergencies.
  - 2. At least three bids must be taken and documented.
  - 3. When practical, the city purchasing office will handle the buying of items needed by the department.
- D. Purchases costing \$3,000 to \$49,999.99 will be purchased on a competitive bid basis. A bid will be awarded to the lowest responsible bidder conforming to specifications and delivery requirements after review by the purchasing office and the issuance of a requisition.
- E. All purchases of \$50,000 or more will be on a competitive, sealed-bid basis, received by the city and referred to the city council for a decision. Requisitions of or above this amount will be forwarded to the purchasing division at least 21 days prior to the anticipated need of the material. In cases involving automotive equipment, thirty (30) days advance notice is required.
- F. It is the responsibility of the Chief of Police, or his designee, who authorizes a routine purchase of equipment and later needs to cancel the order to:
  - 1. Immediately notify the fiscal manager of the desire to cancel.
  - 2. Route a formal memorandum to the city purchasing office.
- G. Any employee who makes a purchase of \$50 or less, requiring cash reimbursement, will take the receipt to the petty cash custodian for processing. The petty cash custodian has the authority to approve or disapprove all petty cash expenditures in accordance with established practice.
- H. The petty cash custodian will ensure that the expenditure meets the criteria for use of a payment authorization. If it does, the petty cash custodian will do the following:
  - 1. Complete the authorization form.
  - 2. Attach the receipt(s).
  - 3. Forward the documents to the city finance director's office.
  - 4. Pay the bill or reimburse the employee as indicated.

- I. The Chief of Police must approve all routine repair and maintenance expenditures prior to receipt of the services.

## **X. PROPERTY LOSS AS A RESULT OF POLICE DUTIES**

Note: In no circumstances shall reimbursement exceed \$200.00 for expensive personal items, such as jewelry, dress watches, fashion clothing, and accessories. Otherwise, the criteria for reimbursement will be evaluated based on the criteria below.

- A. It is the responsibility of an employee experiencing a loss of personal property in the line of duty to submit a memorandum that lists the following details:
  1. The circumstances of the incident.
  2. Whether the loss affecting the employee was a result of damaged, lost, or destroyed property.
  3. The value of the property with proper documentation including receipts, age, and condition of the item(s) at the time of the loss, and any other information the employee thinks is relevant. The documentation must be such that a reasonable person could establish fair market value.
- B. It is the responsibility of the chain of command to make a recommendation for or against reimbursing the employee experiencing the loss and to
  1. Recommend a dollar amount for replacement based on:
    - a. Fair market value of the item(s) or equipment.
    - b. Cost replacement for the item(s) or equipment that provides the same purpose.
  2. The Chief of Police, through consultation with the City Administrator, will make the final determination.
- C. Reimbursement will be made only for items that are normally utilized during police duties, such as:
  1. Wristwatches, clothing, footwear, weapons, and any other equipment not supplied by the department.
  2. Reimbursement will not be made for items that are not normally utilized during police duties, such as ornamental jewelry, hats, and expensive watches, clothing, or footwear. Valuable items of this sort are worn at the employee's own risk.
- D. All employees are expected to maintain care and control of city equipment. Claims for personal items lost, stolen, or damaged will be reviewed as to the circumstances surrounding the loss, including whether or not the employee made every reasonable effort to prevent the loss.


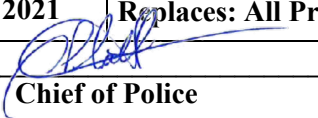
## **XI. AUDITING / ACCOUNTING**

- A. An independent audit of department fiscal affairs is conducted at least annually in connection with the annual city financial audit. The Chief of Police may order an internal audit any time it is deemed necessary to assure accountability.
- B. The Chief of Police will cause an inspection of the petty-cash account transactions on a random or required basis. The inspection will include a review of the formal and informal procedures of each area of fiscal management.
- C. The departments accounting system will include a monthly status report that will be accomplished by the custodian of each account showing:
  - 1. Initial appropriation for each account.
  - 2. Balance at the commencement of the monthly period.
  - 3. Expenditures and encumbrances made during the period.
  - 4. Unencumbered balance at the end of each period.

## **XII. ACCOUNTABILITY OF DEPARTMENTAL CAPITAL EQUIPMENT (TEXAS BEST PRACTICES: 1.10)**

- A. All agency property is inventoried when received. The Chief of Police, or his designee, will be responsible for issuing agency-owned property to authorized users. This includes recovering said property if required when the employee leaves the department.
- B. Departmental capital assets are marked with a property tag if the cost of the item is over \$5000.00, or if their use and life span is more than three years. All department firearms, TASERs, in-car computers, desktop computers, and vehicles (whether bought with city funds or acquired through forfeiture actions) are considered capital assets.
- C. The department will conduct a capital-assets inventory every year and when there is a change in command personnel over a unit or over the entire department. The results of the inventory will be forward to the Chief of Police for review.



	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 1.4 Inspections and Audits</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 1.13, 7.25</b>	

## I. POLICY

Inspections of the department shall be conducted on a regular basis to help ensure that the department is operating at peak efficiency and in compliance with established professional standards. When conducted properly, inspections enable managers to assess the department's ability to perform its mission, provide the information necessary to plan for the improvement of departmental operations, and ensure full capability to perform the department's mission. Inspections are a vital component of departmental self-assessment and as such will be carried out with care, attention to detail, and the full cooperation of all personnel concerned.

## II. PURPOSE

The purpose of this policy is to establish procedures for conducting inspections of the department's administrative functions, facilities, property, equipment, operations, and personnel.

## III. DEFINITIONS

- A. Line Inspection. Line inspections are ones conducted by the supervisory personnel directly responsible for the person, equipment, or facility being inspected. They are designed to examine, evaluate, and improve the performance of departmental personnel and equipment. A written report is not required for a line inspection unless it reveals a critical problem that should be brought to the attention of a higher command level.
- B. Readiness Inspections. A readiness inspection is one conducted to evaluate both equipment and operational readiness of the department to respond to exceptional or emergency circumstances. Such inspections are regularly scheduled but may be initiated at any time at the direction of the Chief of Police or a designee.

## IV. PROCEDURES

- A. Line Inspections
  - 1. Line inspections shall be conducted by the immediate supervisor of the unit or personnel being inspected.

2. Line inspections shall be accomplished at roll call or at such other times as are appropriate for the type of inspection being conducted.
3. Line inspections shall be conducted at least once per week or at such intervals and times as otherwise directed by departmental policy and the supervisor of the unit concerned.
4. Special line inspections may be ordered at any time by the Chief of Police.
5. Line inspections shall, at a minimum, include an examination of each of the following items that are applicable to that unit and that specific inspection:
  - a. Personal appearance and personal hygiene of unit personnel
  - b. Proper wearing of uniforms and uniform equipment
  - c. Health, physical fitness, and fitness for duty of unit personnel
  - d. Appearance and maintenance of department-owned vehicles assigned to or used by that unit
  - e. Unit compliance with departmental policies, regulations, and orders
  - f. Availability and currency of departmental policy and procedure manuals and other departmental publications and documents applicable to that unit
  - g. Physical condition, maintenance, safety, cleanliness, adequacy, and security of the areas, furnishings, and equipment of the portions of the physical plant used by or under the control of that unit
  - h. Such other items as are applicable to the functions of that unit.
6. Inspection Procedure
  - a. Unit supervisors shall conduct informal physical inspections of personnel, equipment, and other items, as directed. Normally no formal written report of line inspections will be required. However, the date of such inspections, items inspected, and condition shall be recorded on a call sheet, and the inspecting supervisor shall document any problems encountered.
  - b. All line inspections shall be conducted in accordance with all appropriate safety precautions.


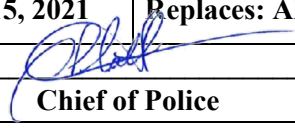
- c. Firearms, both individual and department owned that are used on duty, will be inspected for cleanliness and functionality at least monthly. Firearms and other equipment with the potential for causing injury shall be examined only by persons thoroughly familiar with the item being inspected. Inspection of firearms and other weapons shall be conducted only in a manner consistent with standard safety requirements for the presentation and handling of such weapons.
7. Wherever possible, deficiencies discovered during line inspections shall be corrected immediately by the inspecting supervisor. Where immediate correction is not possible, a re-inspection of the deficient item or personnel shall be conducted as soon as possible to ensure that corrective action has been taken.
8. Repeated failure to correct deficiencies shall be reported to the appropriate authority, and action will be taken to compel compliance by the person or unit responsible for the deficiency. Failure to correct deficiencies may be the subject of disciplinary action.

**B. Readiness Inspections (Texas Best Practices: 7.25)**

1. Equipment readiness inspections will be conducted on all department special-use equipment on a quarterly basis.
2. Each departmental unit will create a checklist of equipment possessed by the unit for special or periodic use. This is typically equipment that is not assigned to individual members of the department. (Emergency Response Team Equipment is covered in Policy 8.4.) Special-use equipment includes special-use vehicles, equipment, or supplies for special events or disasters, or specialized investigative equipment.
3. Checklists should indicate the unit, date inspected, condition of each item, and the person who inspected the equipment. Any maintenance needs will be identified. Copies of each unit checklist shall be forwarded to the Chief of Police for review.

**V. Maintaining Compliance with Texas Law Enforcement Best Practices (Texas Best Practices 1.13)**

- A. The department Senior Sergeant is responsible for ensuring continued compliance with the Texas Law Enforcement Best Practices.
- B. The Senior Sergeant will design and implement a system to ensure all continuing compliance requirements are met and provide immediate feedback to the Chief of Police if a continuing compliance issue is not met.
- C. The Senior Sergeant shall provide the Chief of Police with a memorandum at least monthly advising the status of Best Practices compliance.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 1.5 Mutual Aid</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
<b>Reference:</b>		

## I. POLICY

On occasion the need arises to request assistance from or give assistance to a neighboring law enforcement agency. This need may result from an emergency such as civil disorder, fire, flood, or other disaster, but it is most often requested for backup on calls where officers are at risk and local backup is unavailable. Before the need arises, agencies must clarify and plan emergency procedures. Available county and state support systems shall be used to support operations.

## II. PURPOSE

The purpose of this policy is to establish procedures, duties, and responsibilities for assisting or requesting assistance from another law-enforcement agency and to provide for the use of statewide law-enforcement support systems.

## III. PROCEDURE

### A. Jurisdiction

1. Generally, the legal jurisdiction of the department stops at the city limits, as defined by charter and ordinances; however, officers also have authority to act as peace officers in other areas within the state when requested through a properly executed mutual aid agreement. This authority may be used for the following reasons:
  - a. Assisting neighboring law-enforcement agencies, the county sheriff, or the Texas Department of Public Safety in handling emergency calls and at times when they are unable to respond immediately.
  - b. Assisting neighboring law-enforcement agencies, the county sheriff, or the Texas Department of Public Safety when they need assistance in safely completing a task or assignment.

## B. Mutual aid

1. For the purpose of this policy, mutual aid is defined as the assistance given or asked for between the department and other law- enforcement agencies during emergencies. The circumstances that require mutual aid can include one or more of the following situations:
  - a. Enforcement of laws that control or prohibit the use or sale of controlled drugs.
  - b. Any law-enforcement emergency involving an immediate threat to public safety.
  - c. When executing orders for the temporary detention or emergency custody of people for mental health evaluation.
  - d. Any public disaster, such as fire, flood, epidemic, or civil disorder.
2. Mutual aid may be requested from or provided to another law-enforcement agency by the department at the discretion of the on-duty supervisor. However, officers must remember that they are primarily responsible for providing law-enforcement service to their own jurisdiction. There are generally three levels of mutual aid assistance as follows:
  - a. Short duration, approximately 30 minutes or less, where an additional show of force, backup, traffic control, or assistance with prisoner transportation is required.
  - b. Medium duration, approximately one to four hours, where the senior officer on duty may provide or request assistance from the neighboring law-enforcement agencies, the county sheriff, or Texas DPS; however, their role is normally confined to a show of force, backup, transporting prisoners, or traffic control.
  - c. Long duration, more than four hours, when full-scale assistance is required. The on-duty supervisor shall immediately notify the chief of police who will assist in coordinating additional aid as required.
3. Any mutual aid support between the department and neighboring law- enforcement agencies shall be coordinated in advance through a written agreement. A list of cities with existing mutual aid agreements can be found in the city emergency action plan and in the communications center.
4. Mutual aid agreements shall be reviewed annually to ensure compliance with national incident management system requirements.
5. When taking law-enforcement actions at an emergency site, including uses of force, officers from this department shall at all times adhere to this department's policies and procedures and utilize only those weapons and tactics that they have been trained and deemed qualified to use.

6. Occasionally it is necessary to request assistance from a federal law-enforcement agency, such as when a major crime has occurred, and the suspect may have left the state. The Chief of Police shall decide whether or not to notify the FBI or other appropriate agency.
7. If the department, with the help of neighboring law-enforcement agencies and DPS, is unable to cope with an emergency, such as a riot or other civil disturbance, the chief may contact the governor's office for National Guard assistance.


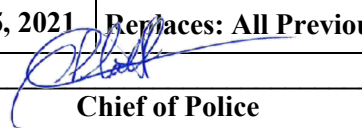
C. Statewide law-enforcement support.

1. The department is a member of and participates in the use of the Statewide Interdepartmental Radio System (SIRS) and complies with the procedures for its use. A copy of these procedures can be found posted in the department communications office.
2. The department participates in the use of the Texas Crime Information Center (TCIC) and complies with the procedures for the use of this exchange. In addition, the department participates in the Uniform Crime Reporting system administered by the Texas Department of Public Safety.
3. Some state-owned law-enforcement resources may be made available to the department for special use. These resources, and the state agency to contact, include:
  - a. Special Weapons and Tactics (SWAT) teams.
  - b. Canine teams —DPS. Canine teams, if requested, shall be used only to track, and great caution shall be used in deploying teams in heavily populated or congested areas. Handlers are responsible for compliance with their own agency policies and procedures.
  - c. Helicopter or fixed-wing aircraft: DPS. Normally the Chief of Police requests the use of this equipment in advance from the DPS director. The equipment may be available on an emergency basis.
  - d. Polygraph: DPS
  - e. Riot truck and equipment: DPS.
  - f. Bomb disposal: DPS.

D. State law-enforcement assistance during declared emergency or disaster situations

1. Only the governor has the authority to provide state law-enforcement assistance during an emergency or disaster situation. State equipment and personnel can be used to support local emergencies or to protect life and property in natural disasters per the governor's authorization. The Chief of Police shall request the mayor to contact the governor in the event state law-enforcement assistance is required.

2. During declared emergencies and disasters, the support listed in section C above is requested through the mayor in the regular NIMS process.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 1.6 Departmental Reports</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
	<b>Reference:</b>	

## I. POLICY

The department is required to maintain records of operations for purposes of investigation and the prosecution of offenders. Records that concern the internal operations of the department must also be kept. It is the intent of the department to provide a reporting system through which quality management and administrative decisions may be made.

## II. PURPOSE

The purpose of this policy is to describe the periodic reports and records prepared by the department and their retention schedules.

## III. ADMINISTRATIVE REPORTS

- A. **Monthly Report:** The department will provide a monthly report to the Chief of Police and the City Administrator. This report contains information specified by the Chief of Police.
- B. **Monthly National Incident Based Report System (NIBRS):** A monthly NIBRS report is compiled by the records supervisor or designee and a copy provided to the Chief of Police for review. The NIBRS report is submitted to the Texas Department of Public Safety (TDPS) via electronic submission through the TDPS Secure Site.
- C. **Annual Report:** The annual report is compiled by the Chief of Police. The report contains an annual summary of the monthly report information and other information that is required by both policy and law. The annual report is forwarded to City Administrator for presentation to the city council.

The annual report is used to determine the following:

- 1. Personnel allocation
- 2. Police patrol district boundaries
- 3. Police staffing levels



4. Statistical information on other related activities and problems.

#### **IV. POLICE RECORDS**


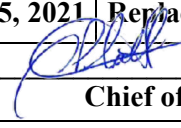
A single sequential incident number is assigned to each incident report, offense report, or accident report made by this department. The number is unique to each incident to ensure the efficient recovery of the report.

#### **V. DESTRUCTION AND RETENTION OF RECORDS**

Texas state law provides a criminal penalty for willful destruction, mutilation, or alteration of public information. Destruction or removal of documents and records of the department shall be made only in accordance with the city's records retention schedule.

#### **VI. DEPARTMENTAL FORMS**

- A. The department shall develop standard forms to be used by officers to assure uniform and consistent reporting of enforcement and enforcement related activities, and to satisfy the requirements of state and federal agencies.
- B. Departmental forms may be created by the unit needing the form, if a form does not yet exist. Any personnel in the department may suggest revisions to an existing form or propose a new form. Proposals and suggestions are submitted to the employee's supervisor. In creating a new form or revising an existing one, care must be exercised to make sure that the new or revised form in no way conflicts with any city policies or other forms.
- C. The Chief of Police must approve all departmental forms.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 1.7 Departmental Goals and Objectives</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 _____ <b>Chief of Police</b>
	<b>Reference:</b>	

## I. POLICY

The City of Teague constructs a long-term strategic plan that outlines the organizational goals and objectives over a three to five-year period. The City Administrator and the Board of Aldermen develop this strategic plan with input from the department directors and the community. Each September, the city manager will update the strategic plan by eliminating goals that have been accomplished and adding new goals that have been developed.

## II. PURPOSE


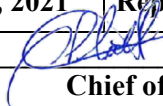
The purpose of this policy is to outline the process used by departmental personnel in the development of departmental goals and objectives.

## III. ANNUAL GOALS AND OBJECTIVES

- A. Each October, after the revision of the strategic plan, the Chief of Police will develop annual goals and objectives for the department. This one-year plan will consist of those goals in the strategic plan that are identified for accomplishment that year plus any additional department-specific goals that need to be addressed.
- B. The Chief of Police shall forward a report on the accomplishment of the previous year's goals to the city manager by the first of November each year.
- C. Each supervisor is responsible for ensuring that all personnel under his/her command are given the opportunity to provide input to the goals, objectives, and strategies of each organizational component.
- D. Upon completion, the one-year plan is to be distributed to all departmental personnel. It is the responsibility of each supervisor to ensure that all personnel under the supervisor's command receive the goals, objectives, and strategies of their organizational component.
- E. The Chief of Police reviews semi-annually, with the supervisory staff, the progress in attaining the goals, objectives, and strategies of each organizational component.

#### **IV. INDIVIDUAL PERFORMANCE PLANS**

Supervisors, when developing individual performance plans for subordinate employees, will include elements of the annual goals and objectives that each employee is expected to assist in accomplishing.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 2.0 Rules of Conduct</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 1.08, 2.02, 2.12, 2.14, 2.15, 2.16, 2.17, 2.18, 2.19, 2.20, 2.21, and 2.22	

## I. POLICY

The Teague Police Department, and the citizens we serve, expect all personnel to maintain high standards of appearance and conduct. The mission of the department is to work with all members of the community to preserve life, maintain human rights, protect property, and promote individual responsibility and community commitment.

## II. PURPOSE

The purpose of this policy is to define departmental expectations for on and off-duty personal behavior. This order applies to all employees both sworn and non-sworn. (Texas Best Practices: 2.12)

## III. CODE OF ETHICS (Texas Best Practices: 2.02)

All officers shall display the integrity required by the Law Enforcement Code of Ethics:

As a law enforcement officer my fundamental duty is to serve the community; to safeguard lives and property; to protect the innocent against deception, the weak against oppression or intimidation, and the peaceful against violence or disorder; and to respect the constitutional rights of all to liberty, equality, and justice.

I will keep my private life unsullied as an example to all and will behave in a manner that does not bring discredit to me or my agency. I will maintain courageous calm in the face of danger, scorn, or ridicule; develop self-restraint; and be constantly mindful of the welfare of others. Honest in thought and deed in both my personal and official life, I will be exemplary in obeying the law and the regulations of my department. Whatever I see or hear of a confidential nature or that is confided to me in my official capacity will be kept ever secret unless revelation is necessary in the performance of my duty.

I will never act officiously or permit personal feelings, prejudices, political beliefs, aspirations, animosities, or friendships to influence my decisions. With no compromise for crime and with relentless prosecution of criminals, I will enforce the law courteously and appropriately without fear, favor, malice, or ill will, never employing unnecessary force or violence and never accepting gratuities.

I recognize the badge of my office as a symbol of public faith, and I accept it as a public trust to be held so long as I am true to the ethics of police service. I will never engage in acts of

corruption or bribery, nor will I condone such acts by other law enforcement officers. I will cooperate with all legally authorized agencies and their representatives in the pursuit of justice.

I know that I alone am responsible for my own standard of professional performance and will take every reasonable opportunity to enhance and improve my level of knowledge and competence.

I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession – law enforcement.

#### **IV. DEFINITIONS**

- A. Affirmative Duty: The personal responsibility and obligation of an employee to report wrongdoing rather than providing such information only when requested.
- B. False Report: A report that is not made in good faith, based on information that is known or reasonably likely to be inaccurate; intentionally or negligently ignores exculpatory or mitigating information; or made with the purpose of harassing or wrongly incriminating another employee.
- C. Good Faith: A report that provides allegations concerning an employee who is reasonably believed to have purposely committed a serious violation of departmental policy, procedures, rules, or laws.
- D. Retaliation: Retaliation of the following kinds is designed to serve as retribution against an employee who, in good faith, has filed a complaint against another employee. In the context of this policy, retaliation includes any deliberate, purposeful actions or failures to act, directed against employees that cause, or that could reasonably be expected to cause, physical harm, property damage, significant emotional stress, or otherwise negatively affect another employee's terms or conditions of employment or that could seriously impair the efficiency, safety or effectiveness of that employee, this department, or both. Such adverse actions may take many forms, including but not limited to, bullying; persistent offensive comments, threats, or intimidation; false accusations; isolating; ostracizing; or acts that malign or disparage an individual's reputation.
- E. Serious Acts of Misconduct: Deliberate acts or failures to act that could reasonably form the basis for significant disciplinary action against an employee. Such disciplinary action would be reasonably likely to adversely affect that employee's terms or conditions of employment up to and including termination of service.

#### **V. GENERAL DUTIES**

- A. All officers shall, within jurisdictional limits, prevent crime, preserve the peace, protect life and property, detect and arrest violators of the law, and enforce the laws of the United States, the laws of the State of Texas, and all local ordinances, according to the rules, regulations, and general orders of the department. Officers must know that when they act under color of law, they are enforcing the law according to statutes, written administrative guidance in the department, ordinances, common usage, and custom. Further, officers shall exhibit good moral character in the administration of their duties according to departmental orders.
- B. The department maintains the right to establish oral and written orders to govern and control the efficiency, effectiveness, and safe operation of law enforcement. Officers shall be trained in the rules and expectations of professional conduct prior to assuming law enforcement duties.
- C. The Teague Police Department and City of Teague reserves the prerogative to discipline personnel for violations of the rules listed in this order as well as violations of all other departmental orders and directives. The decision to discipline and the measure of discipline employed depend on the rule or law violated, the consequences of the employee's actions, and the employee's prior history and experience.
- D. Duty to Report
  - 1. All employees of this department have an affirmative duty to report serious acts of misconduct or failures to perform actions, defined in departmental policy, procedures, and rules. Failure to report shall result in corrective or disciplinary action.
  - 2. Acts of retaliation against employees who make good faith complaints or disclosures of misconduct against another employee are strictly forbidden. Such acts will form the basis for charges of misconduct resulting in serious disciplinary action.
  - 3. All employees have an affirmative duty under this policy to cooperate fully during the investigation of any allegation of employee misconduct, whether conducted by this department or another authorized authority. Protection from retaliation is extended under this policy to all employees who cooperate in good faith.
  - 4. All complaints of retaliation shall be submitted to any supervisor. If the supervisor is the subject of or is involved in the complaint, an employee shall submit the complaint to the next higher-ranking employee in the chain of command.
  - 5. In uncommon situations involving highly egregious offenses or illegality that may have departmental or governmental implications, a complaint may be made directly to the City Administrator for the City of Teague. Examples include but are not limited to broad-based corruption, conspiracy among employees, or offenses involving or including high-ranking officers or members of government.

## **VI. PERFORMANCE PROHIBITIONS**

- A. As appropriate, disciplinary action may be taken for any of the following reasons:
1. Incompetent or inefficient performance or dereliction of duty.
  2. Insubordination, discourteous treatment of the public or a fellow employee, or any act of omission or commission of similar nature that discredits or injures the public. (Insubordination may also consist of direct, tacit, or constructive refusal to do assigned work.)
  3. Mental or physical unfitness for the position that the employee holds.
  4. Conviction of a felony or misdemeanor involving conduct amounting to moral turpitude (see III), or a pattern of misconduct as displayed by a series of misdemeanor convictions.
  5. Failure to report to an appropriate superior authority incompetence, misconduct, inefficiency, neglect of duty, moral turpitude, or any other form of misconduct or negligence of which the employee has knowledge.
  6. Failure of a supervisory employee to take corrective action regarding employees under his or her supervision who may be guilty of any form of neglect of duty or misconduct where the supervisor knows or should have known of the dereliction.
- B. Nothing in these rules and regulations limits the charges against employees because the alleged act or omission does not specifically appear in this manual, other orders, or policies of the department, or in the laws or ordinances that the department has the responsibility to enforce.
- C. No member of the department shall be a member of any organization that advocates the violent overthrow of the government of the United States, the State of Texas, or any unit of local government.
- E. No department member shall participate in any organization that has as its purpose, aim, objective, or has any practices that are contrary to the obligations of a law-enforcement officer under these rules and regulations.
- F. No department member shall participate or align with any organization that advocates discrimination against any person based on sex, color, creed, religious beliefs, national origin, or handicap.

## **VII. Obedience to Rules of Conduct, laws, and orders**

All employees, regardless of rank or assignment, shall be governed by the following general rules of conduct. Violation of any of these rules by any officer of the department shall be considered sufficient cause for dismissal, demotion, suspension, or other disciplinary action.

- A. Obedience to Laws. Employees shall abide by the laws of the United States and the State of Texas as well as the ordinances of the City of TEAGUE.

- B. Adherence to Departmental Rules. Employees shall abide by the rules of the City Personnel Policies, the Teague Police Department Policy and Procedures Manual, and other properly issued internal directives of the Police Department.
- C. Applicability of Rules. Certain rules may not apply in undercover police assignments specifically authorized by supervisors in accordance with this Policy Manual. Officers will be strictly accountable for justifying their actions.
- D. Insubordination. Employees shall promptly obey all lawful orders and directions given by supervisors and radio dispatchers. The failure or deliberate refusal of employees to obey such orders shall be deemed insubordination and is prohibited. Flouting the authority of a supervisor by displaying obvious disrespect or by disputing his or her orders shall likewise be deemed insubordination. (Texas Best Practices: 1.08)
- E. Issuance of Unlawful Orders. No commanding or supervisory employee shall knowingly or willfully issue an order that violates a federal or state law, a city ordinance, or a departmental rule or policy.
- F. Obedience to Unjust or Improper Orders. An employee who receives an order he/she believes is unjust or contrary to a departmental General Order or rule must first obey the order and then may appeal the order to the Chief of Police via the proper chain-of-command.
- G. Obedience to Unlawful Orders. No employee is required to obey an order that is contrary to the laws of the United States or the State of Texas or the ordinances of the City of Teague. An employee who receives an unlawful order shall report in writing the full facts of the incident and any action taken to the Chief of Police via the chain-of-command.
- H. Conflicting Orders. If an employee receives an order that conflicts with one previously given by a supervisor, the employee receiving the order shall respectfully point this out to the supervisor who gave the second order. If the supervisor giving the second order does not change the order in a way that eliminates the conflict, the second order shall stand and shall be the responsibility of the second supervisor. If the second supervisor so directs, the second order shall be obeyed first. Orders shall be countermanded only when necessary for the good of the department. (TEXAS BEST PRACTICES: 1.08)

## **VIII. Attention to Duty**

- A. Performance of Duty. Employees shall always be attentive to their duties, and shall perform all duties assigned to them, even if such duties are not specifically assigned to them in any departmental rules or procedures manual.
- B. Duty of Supervisors. Supervisors will enforce the rules, regulations, and policies of the Teague Police Department. They will not permit, or fail to prevent, violations of the law, departmental rules, policies, or procedures. They will report violations of departmental rules, policies, or procedures to their immediate superior without delay. Where possible, they will actively prevent such violations or interrupt them as necessary to ensure efficient, orderly operations.



- C. Conduct and Behavior. Employees whether on-duty or off-duty shall follow the ordinary and reasonable rules of good conduct and behavior and shall not commit any act in an official or private capacity tending to bring reproach, discredit, or embarrassment to their profession or the department. Employees shall follow established procedures in carrying out their duties as police officers and/or employees of the department and shall, always, use sound judgment.
- D. Responsibility to Serve the Public. Employees shall promptly serve the public by providing direction, counsel, and other assistance that does not interfere with the discharge of their duties. They shall make every attempt to respond personally to the inquiry or request for assistance.
- E. Responsibility to Respect the Rights of Others. Employees shall respect the rights of individuals, and shall not engage in discrimination, oppression, or favoritism. Employees shall maintain a strictly impartial attitude toward all persons with whom they come into contact in an official capacity. (TEXAS BEST PRACTICES: 2.17)
- F. Truthfulness. Members shall be truthful in all official verbal and written communications and reports. Employees will be truthful in any court related testimony or agency investigations. (TEXAS BEST PRACTICES: 2.14) Officers who are undercover or conducting interviews or interrogations may find it necessary to provide inaccurate information to maintain their cover or determine the truthfulness or veracity of a subject.
- G. Officers Always Subject to Duty. Officers shall, always, respond to the lawful orders of supervisors, and to the call of individuals in need of police assistance. The fact that they may be off duty shall not relieve them from the responsibility of taking prompt and proper police action or from being recalled to duty as needed.
  - 1. The above shall not be construed to include enforcement of laws of a Class "C" misdemeanor nature or traffic offenses except for breach of the peace, theft, or assault.
  - 2. While off-duty, or in their personal vehicle, officers shall not enforce, or take any police action to enforce Class "C" offenses. They may, however, contact an on-duty officer to handle the matter and act as a witness to the offense.
- H. Officers Required to Act. Except where expressly prohibited, officers are required to take prompt and effective police action conforming to departmental policy with respect to violations of laws and ordinances coming to their attention or of which they have knowledge. Officers shall promptly and punctually perform all official duties. Officers shall render, or cause to be rendered, medical assistance to any injured person.
- I. Reporting for Duty. Employees shall promptly report for duty properly prepared at the time and place required by assignments, training, subpoenas, or orders. Line officers shall remain at their posts or place of assignment until properly relieved by another officer or dismissed by a supervisor. All other officers and employees shall promptly report for duty properly prepared at the time and place required by assignment and shall remain at their post, place of assignment, or otherwise engaged in their duty assignment until

having completed their tour of duty as set by established procedures or dismissed by a supervisor. Employees are subject to emergency recall and shall report for duty during emergencies when so notified by a supervisor or the Chief of Police. (TEXAS BEST PRACTICES: 2.16, 2.22)

- J. Exceptional leave. Employees shall, in situations requiring emergency leave or sick leave, notify their supervisors of the circumstances as soon as possible. If unable to report to work, employees shall notify the on-duty supervisor at least two hours before reporting time.
- K. Remaining Alert to Duty. While on duty or at training, employees shall remain alert and awake, unencumbered by alcoholic beverages, prescription drugs, illegal narcotics, or conflicts arising from off-duty employment. Employees shall notify their supervisor if they are using any prescribed drug, other medication, or medical device that the employee believes (or has been informed by a physician or prescription label) might impair their driving or critical decision-making.
- L. Prohibition of Personal Business while on Duty. While on duty, officers shall not engage in any activity or personal business that would cause them to neglect their duty.
- M. Availability While On-duty. Employees while on-duty shall not conceal themselves except for some authorized police purpose. Employees shall keep themselves immediately and readily available at all times while on-duty. No employee shall disable or otherwise interfere with the GPS programing of their in-car systems.
- N. Assistance to Fellow Officers. An officer shall not display cowardice in the line of duty or in any situation where the public or another officer might be subjected to physical danger. Unless incapacitated themselves, officers shall aid, assist, and protect fellow officers and citizens in time of danger or under conditions where danger might be impending.
- O. Prompt Response to All Calls. Officers while on-duty shall respond without delay to all calls for police service. Calls shall be answered in compliance with normal safety precautions, traffic laws, and departmental policy.
- P. Duty to Report All Crimes and Incidents. Employees shall promptly report all crimes, violations, emergencies, incidents, dangers, hazardous situations, and police information that come to their attention. Employees shall not conceal, ignore, or distort the facts of such crimes, violations, emergencies, incidents, and information.
- Q. Responsibility to Know Laws and Procedures. Employees shall know the laws and ordinances they are charged with enforcing, all departmental orders and rules, and the duties and procedures governing their specific assignments.
- R. Responsibility to Know Districts and Locations. Officers shall know the location and boundaries of their assigned areas. Officers also shall be familiar with the names and general locations of the City of Teague streets and highways and the names and locations of hospitals and major public buildings.

- S. Keeping Posted on Police Matters. Each day while on-duty and immediately upon returning from an absence, employees shall study and become familiar with the contents of recently issued communications and directives.
- T. Sleeping On-duty. Employees must be alert throughout their tours of duty. Sleeping while on-duty is forbidden.
- U. Assisting Criminal Activity. Employees shall not communicate in any manner, directly or indirectly, any information that may delay an arrest or enable persons guilty of criminal acts to escape arrest or punishment, dispose of property or goods obtained illegally, or destroy evidence of unlawful activity.
- V. Reading On-duty. Employees shall not read newspapers, books, or magazines while on-duty and in the public view unless a supervisory officer has assigned such reading.
- W. Studying On-duty. Employees shall not, during their regularly assigned working hours, engage in any studying activity that is not directly related to their current job assignments.
- X. Maintaining Communications. While officers are on-duty or officially on call, they shall be directly available by normal means of communication, or shall keep their office, headquarters, or supervisors informed of the means by which they may be reached when not immediately available.
- Y. Reporting Accidents and Injuries. Employees shall immediately report the following accidents and injuries: all on-duty traffic accidents in which they are involved, all personal injuries received while on-duty, all personal injuries not received while on-duty but which are likely to interfere with performance of assigned duties, all property damage or injuries to other persons that resulted from the performance of assigned duties, and all accidents involving or loss of city equipment whether on or off-duty.
- Z. Report Address and Telephone Number. Employees shall have a working telephone or other means of communication in case of emergency at their residence and shall register their correct residence address and telephone number with the department. Any change in address or telephone number must be reported immediately. Employees issued a city phone shall always keep it charged and in their possession.
- AA. Testifying in Departmental Investigations. When directed by a competent authority to make a statement or furnish materials relevant to a departmental administrative investigation, officers shall comply with the directive.
- BB. Carrying of Firearms. All officers are required to carry sidearms while on-duty or operating departmental vehicles. While off-duty it is strongly encouraged, but not required, for officers to carry weapons. Officers are required to qualify, annually, with any weapons carried on or off duty.

CC. Registration of Firearms. All weapons carried and used by officers in the performance of their official duties must be registered with the department. Required registration information must be kept current.

## **IX. Cooperation with Fellow Employees and Agencies**

- A. Respect for Fellow Employees. Employees shall treat other members of the department with respect. They shall be courteous, civil, and respectful of their superiors, subordinates, and associates, and shall not use threatening or insulting language whether spoken directly to a specific individual, a third party, or a social media, or other electronic format.
- B. Interfering with Cases or Operations. Employees shall not interfere with cases assigned to others. Employees shall not interfere with the work or operations of any unit in the department or the work or operations of other governmental agencies. Employees against whom a complaint has been made shall not directly or indirectly contact or attempt to contact for any reason, the complainant, witness or any other persons related to the case in an attempt to intimidate or to secure the abandonment or withdrawal of the complaint, charges, or allegations.

## **X. Restrictions on Behavior**

- A. Interfering with Private Business. Employees, during their duties, shall not interfere with the lawful business of any person.
- B. Use of Intimidation. Employees shall not use their official positions to intimidate persons.
- C. Soliciting and Accepting Gifts and Gratuities. Unless approved by the Chief of Police, employees of the Teague Police Department may not accept any reward, gratuity, gift, or other compensation for any service performed as a result of or in conjunction with their duties as employees of the department regardless of whether the service was performed while said persons were on or off-duty. Employees also shall not solicit any gift, gratuity, loan, present, fee, or reward. (TEXAS BEST PRACTICES: 2.21)
- D. Soliciting and Accepting Gifts from Suspects and Prisoners. Employees are strictly prohibited from soliciting or accepting any gift, gratuity, loan, fee or other item of value, or from lending or borrowing, or from buying or selling anything of value from or to any suspect, prisoner, defendant or other person involved in any case, or other persons of ill repute, or professional bondsmen, or other persons whose vocations may profit from information obtained from the police department. (TEXAS BEST PRACTICES: 2.21)
- E. Reporting Bribe Offers. An officer who receives a bribe offer shall promptly make a written report to his/her commanding officer. (TEXAS BEST PRACTICES: 2.21)
- F. Accepting Gifts from Subordinates. Employees shall not receive or accept any gift or gratuity from subordinates, other than customary celebratory times such as holidays or birthdays, without approval from the Chief of Police. (TEXAS BEST PRACTICES: 2.21)

- G. Soliciting Special Privileges. Employees shall not use their official positions or identification to solicit special privileges for themselves or others, such as free admission to places of amusement, discounts on purchases, or free or discounted meals or refreshments. (TEXAS BEST PRACTICES: 2.21)
- H. Personal Use of Police Power. Officers shall not use their police powers to resolve personal grievances (e.g., those involving the officer, family members, relatives, or friends) except under circumstances that would justify the use of self-defense, actions to prevent injury to another person, or when a serious offense has been committed that would justify an arrest. In all other cases, officers shall summon on-duty police personnel and a supervisor in cases where there is personal involvement or a conflict of interest that would reasonably require law enforcement intervention.
- I. Giving Testimonials and Seeking Publicity. Employees representing themselves as members of the Teague Police Department shall not give testimonials or permit their names or photographs to be used for commercial advertising purposes. Employees also shall not seek personal publicity either directly or indirectly in the course of their employment.
- J. Soliciting Business. Employees shall not, while on-duty, solicit subscriptions, sell books, papers, tickets, merchandise, or other items of value nor collect or receive money or items of value for any personal gain to themselves or others. Employees may solicit for projects related to charitable fundraising, but only when done in a manner not to disrupt the workplace and only with the approval of the Chief of Police.
- K. Drinking On-Duty. Employees shall not drink any intoxicating beverages while on-duty. (TEXAS BEST PRACTICES: 2.19)
- L. Intoxication. Employees shall not be under the influence of any intoxicating beverage or substance during their tour of duty or immediately prior to their tour of duty. Nor shall officers be intoxicated off-duty while in the public view. While off-duty, officers that have consumed an alcoholic beverage to the extent that their mental and physical faculties are impaired shall refrain from exercising any police authority. Officers assigned to special units, or assignments where they may consume alcoholic beverage during the performance of their duties, shall not do so to the extent that their mental and physical faculties are significantly impaired. (TEXAS BEST PRACTICES: 2.19)
- M. Drinking While in Uniform. At no time shall any officer consume alcoholic beverages while in uniform or wearing departmentally identifiable clothing or items (badges, patches, hats, etc.). (TEXAS BEST PRACTICES: 2.19)
- N. Liquor on Official Premises. Employees shall not bring containers of intoxicating beverages into a Police Department building or vehicle except as evidence. (TEXAS BEST PRACTICES: 2.19)
- O. Entering Bars, Taverns, and Liquor Stores. Officers on-duty or in uniform shall not enter or visit any bar, lounge, parlor, club, store, or other establishment whose primary purpose is the sale and on-premises consumption of liquor, unless for the purpose of official duties, and shall not otherwise enter, remain in, or frequent such places. Officers on-duty

or in uniform shall not purchase intoxicating beverages at any time. (TEXAS BEST PRACTICES: 2.19)

- P. Drug Usage. Employees shall not use any illegal drug, or any controlled drug not prescribed by a physician, while on or off duty. Employees shall notify their supervisor if they are using any prescribed drug, other medication, or medical device that the employee believes (or has been informed by a physician or prescription label) might impair their driving or critical decision-making. (TEXAS BEST PRACTICES: 2.20)
- Q. Tobacco Use. Smoking is prohibited in all office and building areas under departmental control and occupied by department employees, except in designated smoking areas. Smoking use is prohibited in all department or city vehicles. Smoking includes use of electronic cigarettes or similar devices.
- R. Public Tobacco Use Prohibited. Officers shall not smoke or otherwise use tobacco products while in city vehicles, engaged in traffic control, on a call for service or investigation, or while otherwise in contact with or within view of the public.
- S. Playing Games On-Duty. Officers on-duty or in uniform shall not engage in any games of cards, billiards, pool, dominoes, electronic arcade games, portable electronic games, computer games including both internally programmed games, such as solitaire or Internet based games, or other games.
- T. Political Activity. While in uniform or on-duty, officers are not allowed to actively participate in political campaigns (e.g., make political speeches, pass out campaign or other political literature, write letters, sign petitions, actively and openly solicit votes). Civilian employees are not allowed to actively participate (e.g., make political speeches, pass out campaign or other political literature, write letters, sign petitions, actively and openly solicit votes) in political campaigns while on-duty. (TEXAS BEST PRACTICES: 2.15)
- U. Improper Release of Information. Employees shall not communicate to any person who is not an employee of this department any information concerning operations, activities, or matters of law-enforcement business, the release of which is prohibited by law or which may have an adverse impact on law enforcement operations or officer safety. Each employee of Teague Police Department shall sign a non-disclosure agreement to this effect.
- V. Seeking Personal Preferment. Employees shall not solicit petitions or influence or seek the intervention of any person outside the department for purposes of personal preferment, advantage, transfer, advancement, promotion, or change of duty for themselves or for any other person.
- W. Criticism of the Department. Employees shall neither publicly nor at internal official meetings criticize or ridicule the department or its policies, city officials or other employees by speech, writing, or other expression, where such speech, writing, or other expression is defamatory, obscene, bigoted, or unlawful, or if it undermines the

effectiveness of the department or city, interferes with the maintenance of discipline, or is made with reckless disregard for truth or falsity.

- X. **Disruptive Activities.** Employees shall not perform any action that tends to disrupt the performance of official duties and obligations of employees of the department, or which tend to interfere with or subvert the reasonable supervision or proper discipline of employees of the department.
- Y. **Operation and Use of Police Radios.** Operation and use of police radios is restricted to authorized and official police business. Personal conversations, or using vulgar, sarcastic, bigoted, or obscene language, or making unnecessary sounds are not permitted. Use of radios is governed by Federal Communications Commission (FCC), of which employees shall always adhered to those rules and regulations.
- Z. **Use of Racial or Religious Jokes and Slurs.** No employee shall engage in any form of speech likely to be construed as a racial, ethnic, or religious slur or joke, whether in the presence of the public or of other employees.
- AA. **Use of Force.** Officers shall use only that amount of force reasonably necessary to accomplish their police mission.
- BB. **Indebtedness to Subordinates.** Supervisors shall not become indebted to their immediate subordinates.
- CC. **Personal Relationships Prohibited with Certain Persons.** Employees shall not become personally involved or develop a personal or social relationship with a victim, suspect, witness, or defendant while any case is being investigated or prosecuted because of such investigation. (TEXAS BEST PRACTICES: 2.18)
- DD. **Duty to be Kind, Courteous, and Patient.** Employees shall, always, be courteous, kind, patient, and respectful in dealing with the public. Employees shall strive to win the respect of all members of the community in the discharge of their official duties. When addressed, employees shall avoid answering questions in a short or abrupt manner, and shall not use harsh, coarse, violent, profane, indecent, suggestive, sarcastic, bigoted, or insulting language.

## **XI. Identification and Recognition**

- A. **Giving Name and Badge Number.** Officers shall give their name, badge number, and other pertinent information to any person requesting such facts unless doing so would jeopardize the successful completion of a police assignment.
- B. **Carrying Official Identification.** Officers shall always carry their official identification on their persons. All employees will carry their official identification on or about their persons while on-duty.

- C. Personal Cards. Employees are not permitted to have or use personal cards showing their connection to the department if such cards bear any information not directly pertaining to their work as police department employees.
- D. Exchange, Alteration, or Transfer of Badge. An employee's issued badge shall not be altered or exchanged between employees or transferred to another person except by order of the Chief of Police. Employees retiring or resigning will not be permitted to retain their badge when doing so will hamper normal operations of the department. Badges are property of the Teague Police Department and must be returned when employment is terminated.
- E. Plainclothes Officers – Identification. A uniformed officer shall neither acknowledge nor show recognition of another police officer in civilian clothes unless that officer first addresses the uniformed officer.

## **XII. Maintenance of Property**

- A. Use of City Property or Service. Officers shall not use or provide any city equipment or service to another, other than for official city business.
- B. Responsibility for City Property. Employees shall be responsible for the proper care and use of department property and equipment assigned to or used by them and shall promptly report to their supervisors any loss, damage, destruction, or defect therein.
- C. Departmental Vehicles. Employees shall operate department vehicles and other equipment in such a manner as to avoid injury to persons or damage to property. Whenever a police vehicle is involved in an accident, or damage is caused to, the operator shall notify a supervisor immediately. Under no circumstances shall an officer investigate his or her own accident. Employees shall request a Department of Public Safety Trooper be dispatched to investigate any accident involving a department vehicle.
- D. Reporting Damage. At the beginning of a tour of duty, employees shall examine any vehicle assigned to them and report any operational deficiencies, damage, or defects to their supervisors. Failure to report damage or defects creates the presumption that the employee inspected the vehicle and found no damage or defects. The employee, in this case, shall be held responsible for the damage.
- E. Responsibility for Private Property. Employees are responsible for protecting private property or equipment that has come into their possession, by reason of their official duties, against loss, damage, or destruction.
- F. Care of Quarters. Employees shall keep their offices, lockers, and desks neat, clean, and orderly.
- G. Property and Evidence. Employees shall not convert to their own use, manufacture, conceal, falsify, destroy, remove, tamper with, or withhold any property or evidence held in connection with an investigation or other official action except in accordance with established procedures. Any property or evidence coming into the possession of an



employee shall be secured in the departmental evidence system, and chain of custody documented, before the end of shift.

- H. Alteration or Modification of Police Equipment. Officers shall not use any equipment that does not conform to departmental policy or specifications. All equipment shall be carried and utilized only as issued and authorized, and no changes, alterations, modifications, or substitutions shall be made to such equipment unless approved by the Chief of Police.


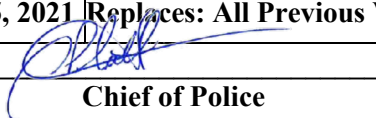
### **XIII. Relationship with Courts and Attorneys**

- A. Attendance in Court. Employees shall arrive on time for all required court appearances and be prepared to testify. Each member shall be familiar with the laws of evidence and shall testify truthfully on any matter.
- B. Recommending Attorneys or Bondsmen. Employees shall not suggest, recommend, advise, or counsel the retention of a specific attorney or bondsmen to any person coming to their attention because of their official duties.
- C. Testifying for a Defendant. Any employee subpoenaed or requested to testify for a criminal defendant or against the City of Teague or against the interests of the department in any hearing or trial shall immediately notify the Chief of Police through the chain of command.
- D. Interviews with Attorneys. Interviews between an officer and a complainant's attorney about a case arising from the officer's employment by the department shall be done in the presence of or with the knowledge and consent of the Chief of Police, department legal counsel, or prosecutor.
- E. Assisting and Testifying in Civil Cases. Officers shall not serve civil-process papers nor render assistance in civil cases except as required by law. No employee shall volunteer to testify in civil actions.
- F. Notice of Lawsuits against Officers. Employees who have had a suit filed against them because of an act performed in the line of duty shall immediately notify the Chief of Police in writing and furnish a copy of the complaint as well as a full and accurate account of the circumstances in question.
- G. Notice of Arrest or Citation. Employees who have become the subject of a citation or arrest action in any other jurisdiction shall immediately notify the Chief of Police.
- H. Arrest of Officer from Another Agency. An officer who arrests a sworn officer of another law enforcement agency shall immediately notify the Chief of Police. Officers shall take whatever action is appropriate to the circumstances including issuance of summonses or making a physical arrest. That the person cited or arrested is a law-enforcement officer shall make no difference.
- I. Arrest of TEAGUE Officer. If an officer has probable cause to arrest a sworn officer of our department, the officer shall first contact his or her immediate supervisor to review and

confirm probable cause. In most cases, the officer may obtain a warrant against the suspect officer. Some occasions may demand an immediate custodial arrest. The Chief of Police shall be immediately notified of all incidents involving any criminal law violations of officers of this department.

#### **XIV. Expectation of Privacy**

- A. Employees shall have no expectation of personal privacy in such places as lockers, desks, departmentally owned vehicles, file cabinets, computers, or similar areas that are under the control and management of this law enforcement agency. While this agency recognizes the need for officers to occasionally store personal items in such areas, officers should be aware that these and similar places may be inspected or otherwise entered—to meet operational needs, internal investigatory requirements, or for other reasons at the direction of the Chief of Police or his/her designee.
- B. No member of this agency shall maintain files or duplicate copies of official agency files in either manual or electronic formats at his or her place of residence or in other locations outside the confines of this agency without express permission from the Chief of Police.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 2.1 Bias Based Policing</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
	<b>Reference: TEXAS BEST PRACTICES 2.01</b>	

## I. POLICY

We are committed to a respect for constitutional rights of all persons in the performance of our duties. Our success is based on the respect we give to our communities, and the respect members of the community observe toward law enforcement. To this end, we shall exercise our sworn duties, responsibilities, and obligations in a manner that does not discriminate based on race, sex, gender, sexual orientation, national origin, ethnicity, age, disability, or religion. Respect for diversity and equitable enforcement of the law are essential to our mission.

All enforcement actions shall be based on the standards of reasonable suspicion or probable cause as required by the Fourth Amendment to the U. S. Constitution and by statutory authority. In all enforcement decisions, officers shall be able to articulate specific facts, circumstances, and conclusions that support probable cause or reasonable suspicion for arrests, searches, seizures, and stops of individuals. Officers shall not stop, detain, arrest, search, or attempt to search anyone based solely upon the person's race, ethnic background, gender, sexual orientation, religion, economic status, age, cultural group, or any other identifiable group.

All departmental orders are informed and guided by this directive. Nothing in this order limits non-enforcement consensual contacts between officers and the public.

## II. PURPOSE

The purpose of this order is to inform officers that bias-based policing is prohibited by the department. Additionally, this order will assist officers in identifying key contexts in which bias may influence these actions and emphasize the importance of the constitutional guidelines within which we operate.

## III. DEFINITIONS

Most of the following terms appear in this policy statement. In any case, these terms appear in the larger public discourse about alleged biased enforcement behavior and in other orders. These definitions are intended to facilitate on-going discussion and analysis of our enforcement practices.

- A. Bias: Prejudice or partiality based on preconceived ideas, a person's upbringing, culture, experience, or education.

- B. Biased-based policing: Stopping, detaining, searching, or attempting to search, or using force against a person based upon his or her race, ethnic background, gender, sexual orientation, religion, economic status, age, cultural group, or any other identifiable group.
- C. Ethnicity: A cluster of characteristics that may include race but also cultural characteristics or traits that are shared by a group with a common experience or history.
- D. Gender: Unlike sex, a psychological classification based on cultural characteristics or traits.
- E. Probable cause: Specific facts and circumstances within an officer's knowledge that would lead a reasonable officer to believe that a specific offense has been or is being committed, and that the suspect has committed it. Probable cause will be determined by the courts reviewing the totality of the circumstances surrounding the arrest or search from an objective point of view.
- F. Race: A category of people of a particular decent, including Caucasian, African, Hispanic, Asian, Middle Eastern, or Native American descent. As distinct from ethnicity, race refers only to physical characteristics sufficiently distinctive to group people under a classification.
- G. Racial profiling: A law-enforcement initiated action based on an individual's race, ethnicity, or national origin rather than on the individual's behavior or on information identifying the individual as having engaged in criminal activity.
- H. Reasonable suspicion: Specific facts and circumstances that would lead a reasonable officer to believe criminal activity is afoot and the person to be detained is somehow involved. Reasonable suspicion will be determined by the courts reviewing the totality of the circumstances surrounding the detention from an objective point of view.
- I. Sex: A biological classification, male or female, based on physical and genetic characteristics.
- J. Stop: An investigative detention of a person for a brief period, based on reasonable suspicion.

#### **IV. PROCEDURES**

##### **A. General responsibilities**

1. Officers are prohibited from engaging in bias-based profiling or stopping, detaining, searching, arresting, or taking any enforcement action including seizure or forfeiture activities, against any person based solely on the person's race, ethnic background, gender, sexual orientation, religion, economic status, age, cultural group, or any other identifiable group. These characteristics, however, may form part of reasonable suspicion or probable cause when officers are seeking a suspect with one or more of these attributes. (TEXAS BEST PRACTICES: 2.01)

2. Investigative detentions, traffic stops, arrests, searches, and property seizures by officers will be based on a standard of reasonable suspicion or probable cause in accordance with the Fourth Amendment of the U.S. Constitution. Officers must be able to articulate specific facts and circumstances that support reasonable suspicion or probable cause for investigative detentions, traffic stops, subject stops, arrests, nonconsensual searches, and property seizures. Except as provided in number 3 below, officers shall not consider race/ethnicity in establishing either reasonable suspicion or probable cause. Similarly, except as provided below, officers shall not consider race/ethnicity in deciding to initiate even those nonconsensual encounters that do not amount to legal detentions or to request consent to search.
3. Officers may consider the reported race or ethnicity of a specific suspect or suspects based on trustworthy, locally relevant information that links a person or persons of a specific race/ethnicity to an unlawful incident(s). Race/ethnicity can never be used as the sole basis for probable cause or reasonable suspicion. Except as provided above, reasonable suspicion or probable cause shall form the basis for any enforcement actions or decisions. Individuals shall be subjected to stops, seizures, or detentions only upon reasonable suspicion that they have committed, are committing, or are about to commit an offense. Officers shall document the elements of reasonable suspicion and probable cause in appropriate reports.
4. Officers shall observe all constitutional safeguards and shall respect the constitutional rights of all persons.
  - a. As traffic stops furnish a primary source of bias-related complaints, officers shall have a firm understanding of the warrantless searches allowed by law, particularly the use of consent. How the officer disengages from a traffic stop may be crucial to a person's perception of fairness or discrimination.
  - b. Officers shall not use the refusal or lack of cooperation to justify a search of the person or vehicle, or a prolonged detention once reasonable suspicion has been dispelled.
2. All personnel shall treat everyone with the same courtesy and respect that they would have others observe to department personnel. To this end, personnel are reminded that the exercise of courtesy and respect engenders a future willingness to cooperate with law enforcement.
  - a. Personnel shall facilitate an individual's access to other governmental services whenever possible and shall actively provide referrals to other appropriate agencies.
  - b. All personnel shall courteously accept, document, and forward to the Chief of Police any complaints made by an individual against the department. Further, officers shall provide information on the complaint's process and shall give copies of "How to Make a Complaint" when requested or when it is reasonable to assume

3. When feasible, personnel shall offer explanations of the reasons for enforcement actions or other decisions that bear on the individual's well-being unless the explanation would undermine an investigation or jeopardize an officer's safety.
4. When concluding an encounter, personnel shall thank him or her for cooperating.
5. When feasible, all personnel shall identify themselves by name. When a person requests the information, personnel shall give their departmental identification number, name of the immediate supervisor, or any other reasonable information.
6. All personnel are accountable for their actions. Personnel shall justify their actions when required.

#### B. Supervisory responsibilities

1. Supervisors shall be held accountable for the observance of constitutional safeguards during the performance of their duties and those of their subordinates. Supervisors shall identify and correct instances of bias in the work of their subordinates.
2. Supervisors shall use the disciplinary mechanisms of the department to ensure compliance with this order and the constitutional requirements of law enforcement.
3. Supervisors shall be mindful that in accounting for the actions and performance of subordinates, supervisors are critical to maintaining community trust in law enforcement. Supervisors shall continually reinforce the ethic of impartial enforcement of the laws, and shall ensure that personnel, by their actions, maintain the community's trust in law enforcement.
4. Supervisors are reminded that biased enforcement of the law engenders not only mistrust of law enforcement but increases safety risks to personnel as well as exposing the employee(s) and department to liability.
5. Supervisors shall be held accountable for repeated instances of biased enforcement of their subordinates if the supervisor knew, or should have known, of the subordinate's actions.
6. Supervisors shall ensure that all enforcement actions are duly documented per departmental policy. Supervisors shall ensure that all reports show adequate documentation of reasonable suspicion and probable cause, if applicable. Any enforcement action that begins as a consensual encounter will also have the circumstances of the initial encounter documented.
7. Supervisors shall facilitate the filing of any complaints about law- enforcement service.

8. Supervisors will randomly review at least three video recordings per officer (either body camera and/or in-car camera video) per quarter. For this policy, a “quarter” is defined as a 3-month period. Supervisors are not required to watch each incident of an entire shift; however, reviewing the footage in a manner intended to gain an understanding of that officer’s performance and adherence to policy and law is required. Supervisors will document the random review of the video and any violations of policy or law will be addressed using existing internal affairs policy. (TEXAS BEST PRACTICES: 2.01)
9. Section 8 above applies only to first-line uniformed officers and their immediate supervisors. In the absence of a first-line supervisor this responsibility will move to the next ranking supervisor.

C. Disciplinary consequences

Actions prohibited by this order shall be cause for disciplinary action, up to and including dismissal.

D. Training (TEXAS BEST PRACTICES: 2.01)

Officers shall complete all training required by state law regarding bias-based profiling.

## II. COMPLAINTS


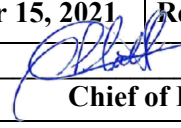
- A. The department shall publish “How to Make a Complaint” folders and make them available at all city facilities and other public locations throughout the city. The department’s complaint process and its bias-based profiling policy will be posted on the department’s website. The information shall include, but is not limited to, the email, physical address, and telephone contact information for making a complaint against an employee. Whenever possible, the media will be used to inform the public of the department’s policy and complaint process.
- B. Complaints alleging incidents of bias-based profiling will be fully investigated as described under Policy 2.4.
- C. Complainants will be notified of the results of the investigations when the investigation is completed.

## III. RECORD KEEPING

- A. The department will maintain all required records on traffic stops where a citation or warning is issued or where an arrest is made after a traffic stop.
- B. The information collected above will be reported to the Board of Aldermen as required by law.

C. The information will also be reported to TCOLE in the required format.



	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 2.2 Sexual or Other Illegal Harassment</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: TEXAS BEST PRACTICES 2.11</b>	

## I. POLICY

The departmental and city’s policy are to provide a professional, businesslike work environment free from all forms of employee discrimination, including incidents of sexual or other forms of illegal harassment, which include color, race, religion, age, and national origin.

No employee shall be subjected to unsolicited or unwelcomed sexual overtures or conduct, either verbal or physical. The harassing behavior, to be subject to this order, need not occur only during work hours on agency premises, but may occur before or after work and at other locations. Sexual or other unlawful harassment, regardless of the type, is misconduct and the department shall apply appropriate disciplinary sanctions.

Two kinds of sexual harassment apply: quid pro quo harassment and hostile work environment harassment, defined below. The two forms of harassment may overlap.

## II. PURPOSE

The purpose of this policy is to define and give examples of sexual and other unlawful harassment, outline prohibited behavior, and describe reporting procedures. (TEXAS BEST PRACTICES: 2.11)

## III. DEFINITIONS

### A. Sexual harassment

The Civil Rights Act of 1964 prohibits discrimination based on color, race, religion, age, national origin, and sex. Sexual harassment is a form of sex discrimination. It is defined as follows:

1. Unwelcome sexual advances
2. Requests for favors
3. Verbal or physical conduct that enters into employment decisions

4. Conduct that unreasonably interferes with an employee's work performance
5. Conduct that creates an intimidating, hostile, or offensive working environment.

B. Quid pro quo harassment. ("Quid pro quo" means "something for something.")

This form of sexual harassment occurs when an employee is being pressured to engage in sexual conduct or else lose a tangible job benefit. This form of harassment usually occurs between a supervisor and a subordinate where the harasser has power to control the employee's work benefits, or working conditions, or promotion prospects. Note that this form of harassment is not limited to express demands for sexual favors, but may be implied by circumstances, e.g., offering an employee a sexually explicit magazine.

Examples of this form of harassment include, but is not limited to, the following:

1. A request for sexual favors, accompanied by implied or overt threats concerning a person's employment status.
2. Promise of preferential treatment in terms of benefits or status.
3. Granting job favors to those who participate in consensual sexual activity or penalizing those who refuse to participate.
4. Unwanted, intentional touching (patting, massaging, rubbing, hugging, pinching).
5. Telephoning or following an employee, during work hours or not, and harassing the employee by requesting sexual favors or in other ways.

C. Hostile work environment harassment

This form of harassment is unwelcome conduct that is so severe or pervasive as to change the conditions of the victim's employment, thus creating an intimidating, hostile, or offensive work environment. Examples of this kind of harassment include, but are not limited to, the following:

1. The employee tolerates unwelcome, pervasive conduct including sexual comments of a provocative or suggestive nature.
2. One employee makes jokes or suggestive remarks intended for and directed to another employee.
3. An employee leaves sexually explicit books, magazines, photographs, or other items where employees will find them.
4. An employee makes unwelcome, demeaning comments (such as talking about physical attributes) to another employee.

5. Ridicule, offensive language, propositions, or other similar actions are directed toward an employee, or more than one employee.
6. An employee makes unwanted, unwarranted, unsolicited off-duty telephone calls and/or contact.
7. An employee leaves signed or anonymous notes or drawings on or in desks, on bulletin boards, in lockers or other places.
8. An employee deliberately singles out women in front of men co-workers (or vice versa) and subjects them to demeaning or derogatory remarks.

#### **IV. PROHIBITED CONDUCT**

- A. Employees shall not commit or participate in any form of sexual or other illegal harassment.
- B. The department considers romantic relationships between supervisors and subordinates potentially non-consensual. Personal relationships between supervisors and subordinates should be brought to the attention of the Chief of Police at the earliest point so that a proper course of action can be determined. Failure to do so may result in discipline.
- C. Supervisors shall ensure that pornographic, demeaning, intimidating, or suggestive photographs, illustrations, cartoons or any other form of suggestive material are not posted or kept in any area of the department, including locker rooms, desks, offices or other locations. Materials of this kind used for investigative purposes shall be properly secured according to evidentiary standards. The material in question may be sexual in nature or insulting to a person based on race, religion, national origin, color, or age.
- D. Supervisors shall order employees on department premises who are making sexually hostile comments or degrading or demeaning remarks about other persons of the same or opposite sex to cease doing so or face discipline.
- E. Employees shall avoid inappropriate physical contact with one another unless required by a training situation or police procedure. Actions such as kissing, back rubbing, embracing, and any other unnecessary touching are prohibited on department premises or while on duty.
- F. Personnel shall not retaliate against any person for reporting sexual harassment, giving testimony, or participating in the investigation. Retaliation in any form shall result in discipline.

#### **V. PROCEDURES**

- A. Employee Responsibilities

1. An employee who believes he or she has been sexually harassed should first tell the offender to cease the inappropriate behavior, although circumstances may not always allow the complainant to make this request. If the conduct does not stop, or if the complainant is unable to confront the offender to stop the action, the complainant shall contact his or her own immediate supervisor. The employee or supervisor shall immediately submit a memorandum to the Chief of Police through the chain of command detailing circumstances. Employees may also report incidents of harassment directly to the Chief of Police or City Administrator if the offender is a higher-ranking member of the department.

If a supervisor learns of an incident of harassment, he or she shall report the matter to the Chief of Police even if the victim did not submit a complaint.

2. If the complainant is not an employee of the department, the complaint itself is considered no less valid and shall be investigated according to the procedures set forth in this order and in Policy 2.4.
3. Employees must understand that sexual harassment can become a criminal matter. Allegations of stalking, assault, and sexual assault shall be handled immediately as criminal investigations.
4. Each employee of this agency is responsible for assisting in the prevention of harassment and discrimination by:
  - a. refraining from participation in or encouragement of action that could be perceived as harassment and/or discrimination.
  - b. reporting observed acts of harassment and discrimination to a supervisor, and
  - c. encouraging any employee who confides that he or she is being harassed or discriminated against to report these acts to a supervisor.
5. Failure of any employee to carry out these responsibilities as defined in this policy will be considered in any performance evaluation or promotional decision and may be grounds for discipline.

#### B. Supervisor Responsibilities:

1. Although all employees shall be responsible for preventing harassment and/or discrimination, supervisors shall be responsible for:
  - a. advising employees on the types of behavior prohibited and the agency procedures for reporting and resolving complaints of harassment and discrimination.


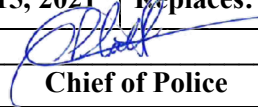
- b. monitoring the work environment daily for signs that harassment and discrimination may be occurring.
  - c. stopping any observed acts that may be considered harassment and discrimination.
  - d. taking appropriate steps to intervene, whether the involved employees are within his/her line of supervision.
  - e. utilizing all reasonable means to prevent a prohibited act from occurring when he or she knows or should know that an employee will or may perform such an activity.
  - f. taking immediate action to prevent retaliation towards the complaining party.
  - g. eliminating the hostile work environment where there has been a complaint of harassment and/or discrimination.
2. No supervisor shall make any employment decision that affects the terms, conditions, privileges, or responsibilities of an individual's employment based on that person's race, sex, religion, national origin, color, sexual orientation, age, or disability.
  3. If a situation requires separation of the parties, care should be taken to avoid action that punishes or appears to punish the complainant.
  4. Transfer or reassignment of any of the parties involved should be voluntary if possible and, if non-voluntary, should be temporary pending the outcome of the investigation.
  5. Any forbidden conduct covered by this policy that comes to the attention of a supervisor shall result in an investigation.
  6. Each supervisor has the responsibility to assist any employee of this agency who comes to that supervisor with a complaint of harassment and discrimination in documenting and filing a complaint.
- C. When an employee reports an allegation of sexual harassment, a confidential internal investigation shall begin immediately.
1. The Chief of Police shall immediately take action to limit the employee(s) involved from any further work contact with the alleged offender.
  2. The Chief of Police shall conduct or cause to be investigated pursuant to the provisions of Policy 2.4.

3. If the sexual harassment allegation is not resolved to the satisfaction of the complainant, eligible employees may invoke the departmental or city grievance procedure.

D. The Chief of Police shall report such allegations to the City Administrator without delay.

## **VI. TRAINING**

The department will provide ongoing training, at least biennially, on sexual and other unlawful harassment, reporting, and investigation procedures.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 2.3 Internal Investigation Process</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> TEXAS BEST PRACTICES 2.04, 2.05, 2.06, 2.07, 2.08, 2.09, and 2.10.	

## I. POLICY

The department's image and reputation depend on the personal integrity and discipline of all departmental employees. To a large degree, the public image of the department is determined by what kind of response the department gives to allegations of misconduct against its employees. The department must competently and impartially investigate all allegations of misconduct by employees and complaints bearing on the department's response to community needs. The department recognizes that its personnel are often subject to intense pressures in the discharge of their duties. The employee must remain neutral under circumstances that are likely to generate tension, excitement, and emotion. In these situations, actions and events frequently result in misunderstanding and confusion. It is to the advantage of all employees to have a procedure for the investigation of the more serious allegations and underlying circumstances so that complaints can be resolved considering the complicated pressures of law-enforcement work.

## II. PURPOSE

The purpose of this policy is to describe the procedure that a citizen must follow in making a complaint against department personnel, to outline the procedure for investigating complaints, and to list and define the dispositions of complaints.

## III. PROCEDURES – GENERAL (TEXAS BEST PRACTICES: 2.04)

### A. Receipt of complaints

The department encourages any person to bring forward grievances regarding misconduct by employees. Department members shall receive all complaints courteously and shall handle them efficiently. All officers are obligated to explain complaint procedures to anyone who inquires.

### B. Responsibilities of supervisors

1. First-line supervisors are primarily responsible for enforcing conformance with departmental standards and orders.
2. First-line supervisors shall know the officers in their charge by closely observing their conduct and appearance.

3. First-line supervisors shall be alert to behavioral changes or problems in their subordinates and, if necessary, document these changes and confer with higher authorities. The first-line supervisor shall assess the behavior and take or recommend appropriate action.
4. The supervisor shall recommend and, if appropriate, help conduct extra training for officers not performing according to established standards.
5. The first-line supervisor shall employ counseling techniques sanctioned by the department. Counseling is used to adjust and correct minor, infrequent errors, or instances of poor performance and to ascertain the nature of any professional or personal problems that bear on performance.
6. The supervisor shall document all instances of counseling.

C. How to make a complaint

A copy of "How to Make a Complaint" will be posted in the public area of the department, provided to media representatives, and given to any person requesting information on how to make a complaint.

D. Responsibility for handling complaints

1. All complaints alleging a violation of the law or policy will be investigated.
2. Complaints regarding law-enforcement operations will usually be handled through the chain of command, beginning with the first-line supervisor.
3. Complaints involving how law-enforcement service is provided or a failure to provide service or improper attitudes or behavior may be investigated by an assigned supervisor or by the Chief of Police.
4. Depending on the nature of the complaint, the Chief of Police may request another agency or DPS to undertake the investigation. (TEXAS BEST PRACTICES: 2.06)

E. Complaint-handling procedures. NOTE: This same procedure can also be used by agency employees who wish to file a complaint against another employee.

1. All complaints, regardless of nature, can be filed in person, by mail, or by phone at any time. As part of the follow-up investigation, persons making complaints by mail or phone normally shall be interviewed and a written, signed complaint prepared.
2. A signed letter of complaint will be accepted as a signed complaint without requiring any specific form.
3. Anonymous complaints shall be followed up to the extent possible. In case of an anonymous complaint, the officer or other person who receives the anonymous complaint shall reduce the complaint to writing in a memorandum with as much information as possible and forward the report to the Chief of Police.



4. Every effort shall be made to facilitate the convenient, courteous, and prompt receipt and processing of any person's complaint. An employee of the department who interferes with, discourages, or delays the making of complaints shall be subject to disciplinary action.
5. Normally, a person with a complaint shall be referred to a supervisor or the Chief of Police, who shall assist the individual in recording pertinent information. If initially reported to a supervisor, the first-line supervisor shall conduct a preliminary investigation. The Chief of Police may, if appropriate, conduct a preliminary investigation. The preliminary investigation consists of questioning the officer, complainants, or witnesses, and securing evidence. Upon completion of the preliminary investigation, the following documents shall be prepared and forwarded through the chain of command:
  - a. a report of the alleged violation
  - b. any documents and evidence pertinent to the investigation
  - c. recommendations for further investigation or other disposition.
6. If the first-line supervisor or other investigators determine that the complainant is apparently under the influence of an intoxicant or drug, or appears to have a mental disorder, or displays any other trait or condition bearing on his or her credibility, the supervisor or investigator shall note these conditions.
7. Any visible marks or injuries relative to the allegation shall be noted and photographed.
8. Prisoners or arrestees also may make complaints. Circumstances may require that a department representative meet the complainant at a jail or prison for an interview. If appropriate, the representative will have photographs taken of any injuries suffered by the complainant.
9. An employee who receives a complaint through U.S. mail shall place the correspondence and envelope in a sealed envelope and forward it to the Chief of Police, who shall determine investigative responsibility.
10. Complaints received by telephone by employees shall be courteously and promptly be referred to a supervisor or the Chief of Police. The employee shall record the name and telephone number of the complainant and state that the Chief of Police or, if unavailable, a supervisor will call back as soon as practical.
11. In every case, the Chief of Police will be notified of any complaint as soon as possible by the supervisor receiving the complaint. Complaints received overnight will be brought to the Chief's attention the next workday. Complaints alleging a violation of the law or any other serious violation should be reported immediately regardless of the time of day. (TEXAS BEST PRACTICES: 2.07)

## F. Disposition of complaints generally

The Chief of Police or his/her designee shall:

1. Notify the complainant, in writing, as soon as practical, that the department acknowledges receipt of the complaint, that it is under investigation and that the complainant will be advised of the outcome.
2. Enter the complaint into the complaint log, assign a complaint number, and have the complaint investigated. Minor complaints alleging rudeness, minor policy violations, and general performance issues may be assigned to a supervisor for investigation and resolution. Allegations of a violation of the law or serious policy violations will be investigated by the Chief of Police, an investigator assigned by the Chief of Police, or an outside agency as determined by the Chief.
3. Maintain complaint files separate from personnel files.
4. Take disciplinary action following the investigation, if appropriate.

## G. Disposition of a serious complaint

1. Allegations of misconduct that might result in discharge, suspension, or demotion, or allegations of criminal charges are serious complaints. The term "serious complaint," in this manual, means that there will be an "internal investigation." Internal investigations examine alleged brutality, gross excesses of legal authority, or allegations involving supervisory or multiple personnel.
2. If a criminal offense is alleged, two separate investigations shall be conducted: a criminal investigation and an administrative or internal investigation. The criminal investigation examines compliance with criminal law while the internal investigation determines compliance with policy and procedure. The Chief of Police will assign these investigations as required.
3. In cases of a serious complaint the Chief of Police shall:
  - a. Determine if the officer complained of should remain on-duty, be relegated to non-contact assignments, or put on administrative leave until the investigation is complete.
  - b. Determine and assign responsibility for the investigation.
  - c. Cause the complaint to be registered and assigned an investigation number in the complaint log.
  - d. Maintain close liaison with the district attorney in investigating alleged criminal conduct. Where liability is at issue, the Chief shall similarly maintain contact with the city attorney or legal counsel.

4. All investigations will be completed within 15 days to include the taking of disciplinary action when necessary. If additional time is necessary to conclude the investigation, a request for extension will be presented to the Chief in writing providing justification for the extension. If the Chief agrees to an extension a specific number of days will be approved. A copy of the request for extension will be provided to the involved officer and the original placed in the case file. (TEXAS BEST PRACTICES: 2.05)
5. Upon completion of any investigation, the Chief of Police will notify the complainant in writing of the results of the investigation and any action taken. (TEXAS BEST PRACTICES: 2.10)

#### **IV. INVESTIGATIVE PROCEDURES**

- A. Two types of investigations may take place: administrative or criminal. Different rules govern interviews of employees in each case.
- B. Assistance of legal counsel
  1. Pursuant Rodriguez v. City of Round Rock Employees do not have the right of having a representative present during administrative investigations or disciplinary hearings.
  2. Employees shall have the right to counsel afforded them during any criminal investigation.
- C. All Interviews
  1. Prior to being interviewed, the subject employee shall be advised of the nature of the complaint and provided a copy of the complaint.
  2. All interviews will be conducted while the employee is on duty, unless the seriousness of the investigation is such that an immediate interview is required, or they are on administrative suspension in accordance with City of Teague and Departmental policy.
  3. During interviews conducted by the department, one employee will be designated as the primary interviewer. Such designation shall be determined by the Chief of Police.
  4. The complete interview shall be recorded. The recording will note the date and time of the interview, who is present at the interview, the time at which breaks are taken in the interview process, who requested the break, the time the interview resumed, and the time the interview was ended.
  5. The employee shall be provided with the name, rank, and command of all persons present during the questioning.
- D. Interviews for criminal investigative purposes

1. If the Chief of Police believes that criminal prosecutions are possible and wishes to use statements against the employee in a criminal proceeding, or at least wishes to maintain the option of their use, he/she or another interviewer shall:
  - a. Give the employee the rights as specified in the Texas Code of Criminal Procedure, Article 38.22 and in accordance with *Miranda v. Arizona*.
  - b. In addition to the rights set forth in state law, the Chief or designee shall advise the employee that if he/she asserts the right not to answer questions no adverse administrative action will be taken based upon the refusal.
  - c. If the employee decides to answer questions at this point, the responses may be used in both criminal and disciplinary proceedings.

E. Interview for administrative purposes

1. If the Chief of Police wishes to compel an employee to answer questions directly related to his or her official duties, the Chief of Police or another supervisor shall advise the employee of the following (Referencing from *Garrity v. New Jersey*, 385 U.S. 483 and *Gardner v. Broderick*, 392 U.S. 273.):
  - a. You are advised that this is an internal administrative investigation only.
  - b. You will be asked and are required to answer all questions specifically related to the performance of your duties and your fitness for office.
  - c. All questions specifically related to employment must be fully and truthfully answered.
  - d. If you refuse to answer these questions, you can be subject to discipline that can be as much as discharge or removal from office.
  - e. Any answers given are to be used solely for internal administrative purposes and may not be used in any subsequent criminal prosecution should such occur.
  - f. The purpose of the interview is to obtain information to determine whether disciplinary action is warranted. The answers obtained may be used in disciplinary proceedings resulting in reprimand, demotion, suspension, or dismissal.
  - g. Information obtained from this interview may not be used for any criminal proceedings.
2. In an interview for administrative purposes, no Miranda rights are required.
3. In an interview for administrative purposes, the employee shall be required to answer questions or risk disciplinary action, up to and including termination, for refusal.

## V. INVESTIGATIVE TOOLS AND RESOURCES

- A. In addition to interviews of the employee and witnesses, other activities in support of a complaint investigation or internal investigation may be required, including:
1. The Chief of Police may order medical and laboratory examinations.
  2. The Chief of Police may, based on reasonable suspicion or his/her observation, require a department employee to submit to a test for alcohol or drug use while on duty. The results may be used in a disciplinary hearing. Refusal to submit to the examination will be grounds for disciplinary action and may result in the employee's dismissal.
  3. If the employee is believed to be under the influence of alcohol, a licensed breathalyzer operator shall administer the test. The Chief of Police shall witness the test and sign the report.
  4. If the employee has a reading of .02 or higher, or there is other competent evidence of impaired abilities to perform duties, the officer shall be relieved of duty by the Chief of Police.
  5. If the employee is believed to be under the influence of self-administered drugs, he/she may be compelled to submit to a blood or urine test. The test shall be administered under medical supervision where hygienic safeguards are met. The sample shall be handled using the same safeguards as evidence in a criminal process.
  6. If the test shows positive results, or there is other competent evidence of impaired abilities to perform duties, the employee shall be relieved of duty as soon as possible by the Chief of Police.
  7. If an employee refuses to submit to a test, (alcohol or drugs) the Chief of Police shall immediately relieve the employee from duty (on paid leave) for failure to cooperate in an administrative investigation and presented to the Board of Aldermen for review and disciplinary actions.
  8. Property assigned to the employee but belonging to the department is subject to inspection if the department has a reasonable suspicion that evidence of work-related misconduct may be found therein. Department property includes files, storage lockers, desks, and vehicles.
- B. Photograph and lineup identification procedures
1. Officers may be required to stand in a lineup for viewing for the purpose of identifying an employee accused of misconduct. Refusal to stand in a properly conducted lineup is grounds for disciplinary action and may result in dismissal.
  2. A book of photos of department employees may be maintained for the purpose of identification of an employee accused of misconduct.

### C. Financial disclosure statements

An employee may be compelled to make financial disclosure statements when directly and narrowly related to allegations of misconduct involving any unlawful financial gain.


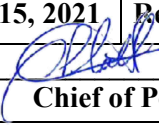
### D. Polygraph

1. All personnel shall be required to submit to a polygraph if ordered to do so by the Chief of Police.
2. The Police Chief may order employees to take a polygraph under the following circumstances:
  - a. The complainant has taken and passed a polygraph concerning the incident, unless the complainant is willing to submit to testing, but the polygraph operator determines the complainant is not a fit subject due to mental condition, age, or medication.
  - b. Regardless of whether or not the complainant takes a polygraph (or is positively identified), and the complaint is of such a nature as to bring severe discredit and suspicion on the department and cannot be satisfactorily resolved in any other manner.
3. The results of the polygraph examination shall not be used as the sole basis for disciplinary action against any employee.
4. Any polygraph examination given under the provisions of this order shall be administered by a private contractor licensed to administer polygraph examinations in the State of Texas or must be a licensed examiner from another law-enforcement agency. No employee shall administer an examination to another employee, regardless of licensing.
5. Refusal to submit to a polygraph examination or to answer all questions pertaining to the charges in the polygraph examination, or deliberately impeding the administration of the polygraph shall be grounds for disciplinary action and may result in dismissal from the department.

## VI. ADJUDICATION OF COMPLAINTS

- A. The Chief of Police will classify completed internal affairs investigations under the following headings:
  1. Unfounded - no truth to allegations.
  2. Exonerated - allegations true but are the result of adherence to departmental policy or procedure. Exonerated complaints will be reviewed by the Chief of Police for consideration of policy revision.
  3. Not sustained - unable to verify the truth of the matter under investigation.

4. Sustained - allegations are true. Complaints will not be classified as sustained unless the finding is based on facts determined during the investigation. (TEXAS BEST PRACTICES: 2.04)
- B. Completed investigations classified as unfounded, exonerated, or not sustained will be maintained in internal affairs files in the Chief's office. Sustained complaints shall be filed in the individual employee's department personnel file and/or their city personnel file, with a copy in the internal affairs files.
  - C. Disciplinary action taken shall be determined by the seriousness of the violation or the extent of injury to the victim, and the officer's prior disciplinary history. It shall be commensurate with the circumstances surrounding the incident, and the employee's service record, including prior sustained complaints, will be considered.
  - D. Disciplinary records (TEXAS BEST PRACTICES: 2.09)
    1. The department shall maintain a log of all complaints.
    2. The complaints and internal investigative files shall be kept in a secure area and shall be maintained in accordance with state law and city policy.
    3. The Chief shall direct a periodic audit of complaints to ascertain a need for training or a revision of policy.

	<b>Teague POLICE DEPARTMENT</b>	
	<b>Policy 2.4 Employee Disciplinary Process</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b>	

## I. POLICY

It is the department's policy to impose any necessary disciplinary action fairly and impartially and to offer adequate appeal procedures to ensure that the rights of employees are protected.

Discipline is the process of taking specific actions that will help train, develop, or modify the inappropriate actions of an employee, preferably through positive rather than negative measures.

Discipline in the department takes two approaches: (1) rewarding employees for excellence and positive actions and (2) training, counseling, and in some cases sanctioning for inappropriate actions or behavior.

## II. PURPOSE

The purpose of this policy is to establish procedures concerning informal and formal disciplinary practices within the department.

## III. DEFINITIONS

- A. Days: The term "days," as used herein, means "workdays provided;" however, if the last day of any time period mentioned is a Saturday, Sunday, or holiday, the time period shall be extended to the next day.
- B. Moral turpitude: An intentional act or behavior displayed in words or actions that violates public morals or the common sense of the community involving but not limited to intent to defraud, intentional dishonesty for personal gain, lying, perjury, subornation of perjury, cheating, bribery, unlawful possession of controlled substances, sexual harassment, unlawful sexual conduct, or excessive use of force.
- C. Relief from duty: An administrative action by a superior whereby a subordinate officer is temporarily relieved from performing his or her duties.
- D. Discipline: The taking of specific actions intended to help train, develop, or modify the actions of an employee. Discipline may be positive (awards and training) or negative (punishment).



## IV. PROCEDURES

### A. Positive Reinforcement

1. Positive discipline seeks voluntary compliance with established policies, procedures, and orders. Methods of positive discipline include:
  - a. Recognition of excellent job performance through rewards or awards.
  - b. When people outside the department compliment an employee's performance, the person who receives the information shall make a record of the comments and pass them to the employee's supervisor. A chief who receives compliments about an employee should write a thank-you note to the individual. Copies of the person's statement and the chief's response shall be sent to the officer involved and the supervisor. A copy of all correspondence shall be placed in the employee's personnel file.
  - c. Truly exceptional acts shall be clearly and promptly identified to the Chief of Police. These acts may be the basis for special awards or for special recognition by community groups or media coverage.
2. Discussion and counseling
3. Training

### B. Consistency in discipline

1. The department abides by the philosophy that discipline must be applied consistently and uniformly.
2. The department provides employees with descriptions of prohibited behavior in the "Rules of Conduct Policy" and elsewhere in these orders. No list, however, can be all-inclusive. Employees are expected to have a reasonable perception of what constitutes proper behavior, based on training and experience.

### C. Relief from duty

1. An employee may be relieved from duty whenever a supervisor, in consultation with the Chief of Police, questions an employee's physical or psychological fitness for duty. An internal investigation may follow.
2. The Chief of Police has authority to relieve an employee from duty, accompanied by a written report setting forth details and circumstances.

3. If the necessity to relieve from duty is not immediate, the behavior or actions of the employee shall be deemed a matter for internal investigation. In an internal investigation, only the Chief of Police may relieve an employee from duty.
4. An officer who refuses to obey a direct order in conformance with departmental policy may be relieved from duty or suspended without pay by the Chief of Police.

D. Penalties: Documented oral reprimand, counseling, and/or training.

1. Oral reprimands resulting from improper actions, while informal, require documentation with an employee's acknowledgment of such record. The following steps shall be observed:
  - a. At the time of an oral reprimand, the employee receiving it shall be counseled as to correct behavior, and further advised that a written record shall be maintained concerning the reprimand/counseling, and that the employee may read the record.
  - b. The employee shall be further advised that he or she has the right to file a statement in his or her personnel file setting forth his or her position, in case of disagreement.
2. The reprimanding supervisor shall prepare a memorandum for the personnel record that contains the following information:
  - a. Employee's name
  - b. Date of reprimand/counseling
  - c. Summary of reasons for reprimand/counseling
  - d. Summary of employee's response
  - e. Suggestions for improvement or specific actions suggested
  - f. Name and signature of counselor
  - g. The following statement must appear:

"I acknowledge that I have today received counseling and I have been advised of the following rights: (1) that a written record of reprimand/counseling shall be maintained; (2) that the employee has a right to review the record and respond in writing; (3) that the form shall become part of the personnel file; and (4) that the employee is required to acknowledge the reprimand/counseling by signing the record."

- h. The employee shall sign and date the form on which the statement appears.
3. Oral reprimand/counseling may involve remedial training. This training may be deemed necessary to rectify the improper behavior. Remedial training may include attendance at academy classes, in-service, or other training specially created to help the employee correct or modify his or her behavior. Remedial training is reasonably offered until the employee can demonstrate proficiency in the correct behavior. All training shall be documented.
  4. If the employee's actions did not result in a formal internal investigation and employee has not behaved improperly following counseling for two years, the record of counseling shall be expunged from the employee's personnel file.
  5. Accumulation of three oral reprimands in a twelve-month period may result in a written reprimand or recommendation for suspension, to the Chief of Police, depending on circumstances.
  6. Supervisors are expected to informally counsel employees regularly without waiting on instances of poor performance. Most counseling is informal, positive, supportive, and often undocumented.
  7. Supervisors are responsible for counseling employees concerning job-related matters within their capabilities. Since many things can affect the job and an employee's performance, job-related counseling may involve family and other individual, personal subjects. Counseling may include identification of unacceptable behaviors or actions, specifically what was done wrong and the desired or acceptable performance. Counseling can attempt to determine the reason for the behavior, determine and recommend how to correct or improve performance or to solve the problem.
- E. Written reprimand. A written reprimand becomes a permanent part of the officer's file.
1. A written reprimand issued by the Chief of Police or a departmental supervisor:
    - a. cautions an employee about poor behavior,
    - b. sets forth the corrected or modified behavior mandated by the department,
    - c. specifies the penalty in case of recurrent poor behavior.

An employee may appeal a written reprimand in writing within ten days of its receipt. The employee may appeal the reprimand to the Chief of Police or City Administrator, who shall be the final arbiter.

#### F. Demotion or suspension without pay

1. If the situation warrants, the Chief of Police may demote, suspend without pay, or take other measures normally considered equivalent against an employee.
2. Suspensions without pay will normally apply to a period of up to 30 days, as determined by the Chief of Police in consultation with the City Administrator.
3. If an employee becomes a candidate for suspension a second time within one year after the first suspension, the employee may be dismissed from employment with this agency, at the discretion of the Chief of Police in consultation with the City Administrator.
4. Suspensions resulting from the arrest or criminal investigation of an employee may be indefinite or result in termination.
  - a. Should an employee be arrested or identified as a suspect in any felony, misdemeanor involving violence or moral turpitude, family violence or DWI, he/she shall immediately be placed on administrative leave with pay and an internal investigation shall commence. At the conclusion of the internal investigation the Chief of Police may take appropriate disciplinary action based on the results of the internal investigation, including indefinite suspension or termination.
  - b. An employee who is acquitted of criminal charges may be or reinstated with full or partial back pay, disciplined at the discretion of the Chief of Police in consultation with the City Administrator.
5. Any employee suspended for a period five days or longer shall return all department-owned property.

On any suspension, the officer must return to department custody his or her badge, identification card, and issued firearm.
6. During a suspension, the employee shall not undertake any official duties.
7. Demotion shall be to the next lowest rank. Demotion shall apply only to the sergeant, senior officer, or K-9 Officer.

#### G. Termination

Terminations are made in cases of extreme misfeasance, malfeasance, or nonfeasance of duty. A complete record of the circumstances of the misbehavior shall be made by all persons having knowledge of the misbehavior.

## H. Reporting arrests

Any employee arrested for, charged with, or convicted of any crime, or required to appear as a defendant in any criminal or civil proceedings must so inform the Chief of Police in writing as soon as possible. Employees do not have to report parking tickets. Employees must report summonses or arrests for reckless driving, DWI, or any other hazardous or moving- traffic offenses. Failure to notify the department of the foregoing shall be cause for disciplinary action.


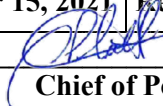
## V. PROGRESSIVE DISCIPLINE

- A. Except for gross breaches of discipline, moral turpitude, or serious violations of law or conduct, the department generally follows the principles of progressive discipline.
- B. Probationary employees shall be dismissed, suspended, or otherwise disciplined according to the foregoing.

## VI. ADMINISTRATION OF SUSPENSIONS, DEMOTIONS, OR DISMISSALS

- A. After an appropriate investigation, should the Chief of Police sustain the allegation and determine that the discipline may be a suspension, demotion, or termination the chief may request review of the investigation by the officer's chain of command to obtain their recommendations for disciplinary action.
- B. Upon receipt of the recommendations, if the Chief of Police believes the discipline should be greater than a written reprimand, the chief shall request that the officer read the written investigation summary and initial each page. The review will take place in the presence of the investigating officer or other staff member. The employee will be allowed to add a written statement to the investigative package stating any arguments with the evidence or investigation process. This statement will be prepared and added to the investigation summary before the employee and the investigating officer leave the review site.
- C. The Chief of Police will meet with the employee and allow the employee to make any statement regarding the evidence or investigation, and review any written statement provided by the employee. The Chief of Police will then have the employee report back after a period determined by the chief.
- D. The Chief of Police will again review the investigation, considering the employee's input and may then decide on the discipline or send the investigation back for further investigation.
- E. The chief will meet with the employee to inform him or her of his/her decision. The chief will present the employee with a letter outlining the discipline, the effective date of the discipline, the reason for the discipline, and the employee's appeal rights.

- F. Copies of all investigation reports that indicate disciplinary action and all other disciplinary paperwork will be filed in the employee's personnel file. A copy of the investigation report will be maintained in the internal investigation files.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 2.5 Accident and Injury Prevention</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: TEXAS BEST PRACTICES 4.10</b>	

## I. POLICY

Motor vehicle crashes involving agency vehicles present serious risks to agency personnel and the public. They also cause considerable financial loss due to injury, loss of manpower, vehicle damage, and possible tort liability. Personnel injuries result in lost time, and in the pain and suffering of our personnel. It is the department's responsibility to minimize these incidents through training, policy development, and review of incidents for compliance with policy. The department will utilize a review process for evaluating crashes and injuries to determine cause and to institute corrective and preventive actions where needed. The reviews and hearings concerning these crashes and injuries shall be conducted according to policy and procedures established herein.

## II. PURPOSE

The purpose of this policy is to provide the authority and operating procedures for review of agency motor vehicle crashes and personnel injuries.

## III. DEFINITIONS

- A. **Motor Vehicle Accident:** For purposes of this policy, a motor vehicle crash is any collision of a vehicle owned by or assigned to this agency with another vehicle, stationary object, or person that results in property damage (regardless of amount) and/or personal injury.
- B. **Personal Injury:** For purposes of this policy, a personal injury is any injury to a member of this department that results in immediate or subsequent treatment by a physician, in lost work time, or one requiring reporting under workers' compensation rules.
- C. **Non-preventable Crash or Injury:** A crash or personal injury shall be classified as non-preventable when it is concluded that the member/operator exercised reasonable caution to prevent the crash or injury from occurring and observed applicable agency policy, procedures, and training.
- D. **Preventable Crash or Injury:** A crash or injury shall be deemed preventable when the member/operator failed to observe agency policy, procedures, or training, and/or failed to exercise due caution or appropriate defensive driving or trained defensive tactics.

## IV. PROCEDURES:

### A. Training

1. The department will provide on-going training to all employees on accident and injury prevention. The Annual Analysis of Accidents and Injuries described in Section E of this order shall be reviewed to identify the training needs of the department.
2. All sworn officers shall complete an emergency driving course at least every three years if their job assignment requires emergency response. A copy of training completion shall be maintained in their training file.
3. All members of the department who drive city vehicles will complete a defensive driving course within six months of hire.

### B. Reporting and Investigating Motor Vehicle Crashes and Injuries.

1. Unless incapacitated, employees are responsible for immediately notifying communications or their supervisor of any motor vehicle crashes, and any personal injury sustained while on duty.
2. Supervisors shall be responsible for ensuring that crash investigations are conducted by an outside agency, preferably Texas Department of Public Safety. The supervisor will also investigate and complete report of injury forms, required by the city's safety policy. Supervisors shall ensure proper medical treatment is afforded an employee involved in an accident.
3. Where feasible, the supervisor, any accident investigators, and the involved officer(s) shall file reports on departmentally approved forms within 24 hours of a crash or injury occurrence.
4. The supervisor shall prepare a memorandum to the Chief that shall include the following information:
  - a. Details of the accident or injury and contributory factors to the crash or injury.
  - b. Statements of witnesses.
  - c. Name and insurance information on involved drivers and others involved in a crash, and the nature/seriousness of injuries and/or property damage.
  - d. A statement as to whether the supervisor believed the employee's injury or crash was "preventable" or "non-preventable"—as defined by this policy—with documentation supporting those conclusions.
  - e. Any recommendations that would help prevent similar crashes in the future.



5. The Chief of Police will review the supervisory investigation and decide whether the accident or injury was preventable or non-preventable.


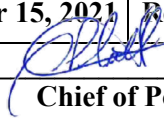
6. Remedial Action

In addition to any other disciplinary measures taken by the department for a violation of policy, the department has the options listed below that can be applied to personnel involved in crashes:

a. Members of the department that have a preventable vehicle crash may be required to undergo additional training, take a defensive driving course, or undergo other corrective measures.

b. Members of the department who have repeated preventable injuries, within a 12-month (1 year) time span, may be terminated due to inability to perform basic job functions in a safe manner.

C. Annually the Chief of Police shall conduct an analysis of all accidents and injuries and make any recommendations for training, equipment, or policy changes needed to reduce employee motor vehicle accidents resulting in property damage and/or personal injuries. The report with its recommendations will be forwarded to the Chief of Police for review and any action necessary.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 2.6 Court Appearance</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
	<b>Reference:</b>	

## I. POLICY

The success of a criminal prosecution is determined not only by the quality and quantity of evidence but by the way it is presented by law enforcement officers in a court of law. An officer's appearance, demeanor, attitude, and ability to testify in a fair and professional manner are essential. Therefore, it is the policy of this agency that officers provide competent and professional testimony by adherence to court scheduling, preparation, appearance, and testimony guidelines provided herein.

## II. PURPOSE

The purpose of this policy is to provide officers with guidelines for scheduling, preparing for, and testifying in criminal court cases.

## III. PROCEDURES

### A. Subpoenas

1. All officers shall accept subpoenas and shall appear in the designated place at the time required. Avoidance of service is strictly prohibited, and offending officers are subject to disciplinary action. This agency shall establish a system of accountability for subpoenas from the point of receipt from the court to the point of officer testimony. This includes but is not limited to:
  - a. recording the receipt of subpoenas to include date received, court date and time, defendant's name, officer's name, and date executed and returned to the court.
  - b. recording the service of subpoenas to named officers by shift supervisors or other designated personnel noting dates received, dates served, and dates returned to the court authority.
  - c. ensuring that notification is made as soon as possible to the designated court authority when officers cannot be served in accordance with established time frames or when they cannot appear on the designated court date.

2. Officers who have been served subpoenas or been given other official notice to appear before a criminal court by means other than the foregoing are responsible for complying with this directive and for providing agency notification as soon as possible of the need for appearance. Such subpoenas shall be recorded in a manner consistent with this policy.
3. Officers who are served with a subpoena shall immediately notify their supervisor and provide the supervisor with a copy.


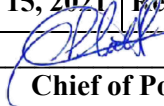
#### B. Preparation for Trial

1. Officers shall fully cooperate with requests from the prosecutor in preparation of cases for trial and may seek pre-trial conferences whenever needed.
2. Officers shall be familiar with the basic rules of evidence and shall seek clarification of any legal issues that may arise during the trial prior to court appearance.
3. Prior to trial, officers designated for court appearance shall review case documentation to ensure that they are completely familiar with the facts involved. In addition, officers shall provide all reasonable assistance necessary to or requested by the prosecution to ensure that necessary evidence will be available at trial.
4. In pretrial conferences with the prosecutor, officers are responsible for providing all information relevant to the case even though it may appear beneficial to the defendant. No detail should be considered too inconsequential to reveal or discuss.
5. If an officer is subpoenaed by the defense in any case, the officer shall immediately notify the Chief of Police and the prosecutor assigned to the case.

#### C. Appearance in Court

1. Officers shall receive compensation for appearance in court during off-duty hours at the rate designated by this agency and in accordance with established means of calculation.
2. Compensation shall be paid only when officers comply with procedures established by this agency for court appearance, including but not limited to supervisory notification/approval and adherence to documentation procedures for overtime pay.
3. Officers who are late for or unable to appear on a court date shall notify the appropriate court authority as soon as possible, providing name, defendant's name, court designation, and reason for absence or tardiness. The reason for absence or tardiness shall be reviewed by the officer's supervisor and may be referred for disciplinary review.

4. Officers' physical appearance, personal conduct, and manner shall conform to the highest professional police standards. All officers shall wear their issued class "A" uniform (Long Sleeve Shirt with Tie and pants without cargo pockets) and have polished black boots/shoes.
5. When testifying, officers shall:
  - a. restrict remarks to that which is known or believed to be the truth
  - b. speak naturally and calmly in a clearly audible tone of voice
  - c. use plain, clearly understood language, and avoid using police terminology, slang, or technical terms
  - d. display a courteous attitude and maintain self-control and composure.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 2.7 Use of Social Media</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b>	

## I. POLICY

Social media platforms provide a new and potentially valuable means of assisting the department and its personnel in meeting community outreach, problem solving, investigations, crime prevention, and other related objectives. The department supports and utilizes the secure and appropriate use of social media to enhance communication, collaboration, and information exchange.

The department also recognizes the role that these tools play in the personal lives of department personnel. Because the improper use of social media platforms by employees may impact department operations, the department provides information of a precautionary nature as well as prohibitions on the use of social media by department personnel.

These policies and procedures apply to all personnel including sworn and non-sworn employees, reserve officers, and any volunteers working with the department.

These policies are in addition to and reinforce that of the City of Teague Social Media Policy contained in the City Policy Manual.

## II. PURPOSE

The purpose of this policy is to establish guidance for the management, administration, and oversight of social media. This policy is not meant to address one form of social media but social media in general, as advances in technology will occur and new tools will emerge.

## III. DEFINITIONS

- A. Blog: A self-published diary or commentary on a topic that may allow visitors to post responses, reactions, or comments. The term is short for “web log.”
- B. Page: The specific portion of a social media website where content is displayed and managed by an individual or individuals with administrator rights.
- C. Post: Content an individual shares on a social media site or the act of publishing content on a site.
- D. Profile: Personal information that a user provides on a social networking site.

- E. Social Media: A category of internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (Flicker, YouTube), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).
- F. Social Networks: Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.
- G. Speech: Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.
- H. Web 2.0: The second generation of the World Wide Web focused on shareable, user-generated content, rather than static web pages. Some use this term interchangeably with social media.
- I. Wiki: Web page(s) that can be edited collaboratively.

#### **IV. DEPARTMENT SPONSORED SOCIAL MEDIA**

##### **A. Requirements for Department Sponsored Public Social Media Sites**

1. The department's Chief of Police is responsible for the management, posting, and monitoring of the department's public social media network sites. Other members of the department may post and monitor specific social media sites as approved by the Chief of Police and City Administrator.
2. The Chief of Police, with input from departmental members will determine the extent of the department's official use of social media platforms. No social media platform will be utilized by the department without the express approval of the Chief of Police and City Administrator.
3. Each social media page for the department shall include an introductory statement that clearly specifies the purpose and scope of the agency's presence on the website and contain the following language:

“This social media account is a limited public forum. As such, any social media content posted must pertain to the scope and purpose of the department's page. A post that contains any of the following material is prohibited and will be removed:

- a. Contains obscene or pornographic material.
- b. Harasses, personally attacks, or threatens another poster.
- c. Endorses or opposes a political campaign, candidate, or measure.
- d. Is unrelated to the purpose and topical scope of the page.
- e. Contains profanity or abusive language; or

- f. Advertises a commercial entity, product, or service”
- 4. Where possible, the page(s) should contain the following information:
  - a. City contact information.
  - b. Link to the City website.
  - c. A statement indicating that all social media content posted on a city or departmental social media account is subject to the Public Information Act, including private messages sent.
  - d. A statement indicating that Public Information Act requests may not be made through social media and providing the email address where an individual should submit a request; and
  - e. “Posted comments do not necessarily reflect the views or position of the City.”
- 5. Social media pages shall clearly indicate that they are maintained by the department and shall have department contact information prominently displayed, where possible.
- 6. Social media content shall adhere to applicable laws, regulations, and policies, including all information technology and records management policies.
- 7. Content is subject to open government laws. Relevant records retention schedules apply to social media content. Content must be managed, stored, and retrieved to comply with open government laws, records retention laws, and e-discovery laws and policies.
- 8. Pages shall clearly indicate that posted comments will be monitored and that the department reserves the right to remove any posting, in accordance with established Social Media policy of the City of Teague.

**B. Operation of Department Sponsored Public Social Media Sites**

Department personnel approved by the department to post to social media outlets shall do the following:

- 1. Always conduct themselves as representatives of the department and, accordingly, shall adhere to all department standards of conduct and observe conventionally accepted protocols and proper decorum.
- 2. Identify themselves as a member of the department.
- 3. Not make statements about the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions, nor post, transmit, or otherwise

disseminate confidential information, including photographs or videos, related to department training, activities, or work-related assignments without express written permission.

4. Not conduct political activities or private business.
5. Department personnel use of personally owned devices to manage the department's social media activities or in the course of official duties is prohibited. No personal devices of any kind are authorized to be used for official business.
6. Employees shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.
7. No employee will delete any posts made by the department, employee, or citizen without approval from the City Administrator/Secretary. The City Administrator/Secretary is the final authority on post deletions on departmental social media sites.

#### C. Uses of Departmental Sponsored Social Media Sites

1. Social media can be used to make time-sensitive notifications related to:
  - a. road closures,
  - b. special events,
  - c. weather emergencies, and
  - d. missing or endangered persons.
2. Social media is a valuable investigative tool and may be used to seek evidence or information about the following:
  - a. missing persons,
  - b. wanted persons,
  - c. gang participation,
  - d. crimes perpetrated online,
  - e. photos or videos of a crime posted by a participant or observer.
3. Social media can be used for community outreach and engagement for the following purposes:
  - a. providing crime prevention tips,
  - b. offering online-reporting opportunities,



- c. sharing crime maps and data
  - d. soliciting tips about unsolved crimes (e.g., Crime Stoppers, text-a-tip).
4. Social media can be a valuable recruitment mechanism since many people seeking employment and volunteer positions use the internet to search for opportunities.
  5. Background investigations.
    - a. This department has an obligation to include internet-based content when conducting background investigations of job candidates.
    - b. Search methods shall not involve techniques that are a violation of existing law.
    - c. Vetting techniques shall be applied uniformly to all candidates.
    - d. Every effort must be made to validate internet-based information that is considered during the hiring process.

#### D. Use of Covert Social Media Sites for Investigative Operations

1. Covert or undercover social media sites are exempt from the requirements of sections 1, 2, and 3 above.
2. Only the Chief of Police may approve the use of any covert or undercover social media site or postings to other social media sites for undercover investigative operations. A supervisor will be assigned to monitor the operation of the investigation.
3. Prior to operating any covert or investigative social media site or posting to other social media sites for purposes of a covert or undercover investigation, the supervisor shall make contact with the prosecuting attorney and the city attorney to determine the admissibility and requirements of the law regarding preservation of information for both prosecution and open government as well as records retention requirements.

## V. PERSONAL USE OF SOCIAL MEDIA

### A. Precautions and Prohibitions

Barring state law or binding employment contracts to the contrary, department personnel shall abide by the following rules when using social media:

1. Members of the department shall adhere to the City of Teague Social Media Policy, contained in the City Policy Manual.
2. Members of the department may not access social networking or social media sites using departmentally provided information systems unless authorized to do so on behalf of the department or during an investigation.

3. Employees are prohibited from authoring posts on a social networking site at any time while on-duty, even during meal breaks.
4. Due to concerns for officer safety and to preserve tactical advantage, the posting of information related to any police response by any officer, or an assisting agency, is absolutely prohibited without the approval of the Chief of Police.
5. All matters of, by, within, and about department details regarding calls for service and the customers we interact with are generally considered confidential information that may not be released, blogged about, posted, or otherwise shared outside the department without prior authorization that has been obtained through an official open- records request, or without the information already being in the public realm [already otherwise released officially].
6. Display of departmental logos, uniforms, uniform patches, or departmental badges on their own or other social media sites is prohibited without written approval of the Chief of Police.
7. Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair working relationships of this department for which loyalty and confidentiality are important, impede the performance of duties, impair discipline and harmony among coworkers, or negatively affect the public perception of the department.
8. As public employees, department personnel are cautioned that speech, whether on or off-duty, made pursuant to their official duties—that is, speech which owes its existence to the employee’s professional duties and responsibilities—may not be protected speech under the First Amendment and may form the basis for discipline if deemed detrimental to the department.
9. Department personnel should assume that their speech and related activity on social media sites will reflect upon their office and this department.
10. Department personnel shall not post, transmit, or otherwise disseminate any information to which they have access because of their employment without written permission from the Chief of Police.
  - a. For safety and security reasons, department personnel are cautioned not to disclose their employment with this department, nor shall they post information pertaining to any other member of the department without that member’s permission. In relation to this, department personnel are cautioned not to post personal photographs or provide similar means of personal recognition that may cause them to be identified as a police officer of this department. Officers who are working, or who may reasonably be expected to work, in undercover operations shall not post any form of visual or personal identification.
  - b. Personnel are reminded that many individuals that we contact in our profession become angry and on occasion seek revenge for official actions taken.


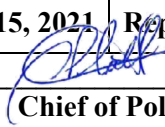
Employees are encouraged not to post any information that could be used to identify an employee's residence, vehicle, or the identity of family members.

11. When using social media, department personnel should be mindful that their speech becomes part of the worldwide electronic domain. Employees are required to be credible witnesses in criminal prosecutions and that credibility can be attacked using inappropriate posts on social media sites. Therefore, adherence to the department's code of conduct is required in the personal use of social media. Department personnel are prohibited from the following:
  - a. Speech containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals.
  - b. Speech involving themselves or other department personnel reflecting behavior that would reasonably be considered reckless or irresponsible.
  - c. Engaging in prohibited speech noted herein may provide grounds for undermining or impeaching an officer's testimony in criminal proceedings. Department personnel thus sanctioned are subject to discipline up to and including termination of office.
  - d. Department personnel may not divulge information gained by reason of their authority; make any statements, speeches, appearances, and endorsements; or publish materials that could reasonably be considered to represent the views or positions of this department without express authorization.
  - e. Department personnel should be aware that they may be subject to civil litigation for the following:
    - i. publishing or posting false information that harms the reputation of another person, group, or organization (defamation).
    - ii. publishing or posting private facts and personal information about someone without that person's permission that has not been previously revealed to the public, is not of legitimate public concern, and would be offensive to a reasonable person.
    - iii. using someone else's name, likeness, or other personal attributes without that person's permission for an exploitative purpose.
    - iv. publishing the creative work of another, trademarks, or certain confidential business information without the permission of the owner.
12. Department personnel should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the department at any time without prior notice.

13. Department personnel should be aware that privacy settings and social media sites are constantly in flux, and never assume that personal information posed on such sites is protected.
14. Department personnel are reminded that the department policies and Code of Conduct applies to on-line activities.
15. There should be no expectation of privacy for items or activities conducted on-line.

B. Monitoring of Social Media

1. Supervisors within the department may make random investigations into the postings of employees for purposes of protecting the integrity and reputation of the department, protecting the integrity of investigations, and ensuring privacy and security of departmental records and information.
2. Any employee becoming aware of or having knowledge of a posting or of any website or web page in violation of the provision of this policy shall notify his or her supervisor immediately for follow-up action.
3. No supervisor or member of the department below the rank of Chief of Police is authorized to cancel, modify, or make exceptions to the contents of this order at any time.

	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 3.0 Basic Training Requirements</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____ <div style="text-align: center;">   <b>Chief of Police</b> </div>
	<b>Reference:</b> TEXAS BEST PRACTICES 1.09, 3.05, 3.06, 3.07, 3.08, 3.09, 3.18, and 8.11.

## I. POLICY

Today’s society is both multi-faceted and complex. To provide effective law enforcement services, it is imperative that officers as well as non-sworn employees have the training necessary to accomplish their mission. The Teague Police Department is committed to providing the training necessary to meet and exceed Texas state requirements and contribute to every employee’s career goals.

## II. PURPOSE

The purpose of this policy is to provide members of the department with details of the training required by the department and their responsibilities regarding maintaining that training.

## III. REQUIRED TRAINING

### A. Basic Training

1. Sworn members of the department are required to have a peace officer license issued by the Texas Commission on Law Enforcement. This license currently requires officers to attend a basic peace officer course and pass a commission licensing examination. Officers must possess their peace officer license prior to performing any law enforcement duty or function. (TEXAS BEST PRACTICES: 1.09)
2. Previously licensed officers who apply for employment must have their license in good standing, all in-service training completed, or the ability to complete in-service requirements prior to the end of the Commission training cycle, which ends August 31 of odd-numbered years.
3. In addition to the training required for licensing, all sworn officers and reserve officers will complete the National Incident Management System training, appropriate for their rank, prior to completion of field training, or prior to completion of promotional probation in the event of promotion to a higher rank. (TEXAS BEST PRACTICES: 8.11)

### B. Field Training

1. All sworn members of the department are required to complete the department’s field training program as outlined in Policy 4-2 within the period specified.

2. Officers with prior experience may qualify for expedited field training if they are able to demonstrate proficiency in all required areas.

C. In-service training (TEXAS BEST PRACTICES: 3.06)

1. All sworn personnel of the department shall, within each Commission training period as required by law, obtain at least 40 hours of in-service training. In-service instruction may include the following:
  - a. A review of changes or revisions in Texas state law
  - b. Training required by the legislature during each four-year training cycle
  - c. Specialized training required at the direction of the Chief of Police or the Commission based on assignment
  - d. Supervisory training
  - e. Policies and procedures
  - f. Firearms training and qualifications (each year).
2. In each two-year cycle, sworn officers must receive the following training:
  - a. Hands-on arrest and/or defensive tactics training
  - b. Initial or refresher self-aid /buddy aid training
  - c. Initial or refresher implicit bias training
  - d. Initial or refresher force avoidance training (de-escalation training)
  - e. Initial or refresher crisis intervention training
  - f. Initial or refresher mental health training
3. Sworn personnel are responsible for obtaining the training necessary to maintain their license and any special certifications they may hold. The department will provide officers with the training or provide the time and funding necessary to obtain the training. Much of the required training can be obtained on-line from the Commission website.
4. Reserve officers will meet the same in-service training requirements as regular officers. (TEXAS BEST PRACTICES: 3.07)
5. The Chief of Police has specific training requirements established by the commission and shall be adhered to. These requirements differ from that of other officers.

D. Supervisory training (TEXAS BEST PRACTICES: 3.09)

All employees, sworn or non-sworn, when promoted to any supervisory rank will be provided supervisory training appropriate to their rank and position within 12 months of their promotion.

E. Civilian personnel (TEXAS BEST PRACTICES: 3.08)

1. All newly appointed civilian personnel will receive the following training from the Chief or his/her designee:
  - a. Orientation to the department's role, purpose, goals, policies, and procedures
  - b. Working conditions, rules, and regulations
  - c. Responsibilities and rights of employees.
2. Non-sworn communicators and communications supervisors will complete Commission's basic tele-communicators and TCIC/NCIC full operators training within 90 days of hire date, along with other required departmental training. (TEXAS BEST PRACTICES: 3.18)
3. Records personnel or personnel assigned to records processing will complete a course in Texas state open records and records retention within 90 days of hire.
4. Any non-sworn personnel who have state-required or job-specific training will be provided that training either prior to job assignment or 180 days.

#### IV. TRAINING EXPECTATIONS

A. Attendance

Personnel are expected to attend all assigned training programs. Attendance will be documented either by the instructor or, in cases where the training is at a location other than the department, documentation will be furnished by those responsible for the training. In some cases, attendance at a training program may be excused, such as for court appearance or sickness. Any absence must be properly excused by the administrators of the program. Any time lost must be made up before any certificate of completion is issued. Certificates will be issued to those students completing training programs. Employees shall provide a copy of any certificates to the department for inclusion in the employee's training file.

B. Expenses

Except for paper and pencils or pens, all expenses incurred by department personnel because of required training will be reimbursed based on actual expenses (receipts must be provided). The city provides per diem to cover the expense of meals, under certain circumstance. A request for per diem must be made at least two weeks before the training event, to allow bookkeeping staff ample time for processing of such requests.

## V. DEPARTMENTAL TRAINING

### A. Performance-based training

The Commission requires performance-based training. This method of training requires the development of performance objectives. The use of performance objectives acquaints the training participants with the information they are required to know, the skills that must be demonstrated, and the circumstances under which the skills will be used. This approach also enables the instructors to relate training directly to the job performance that will be expected by supervisors. An employee who develops an outline for instruction of a topic must develop objectives that have the following characteristics:

1. Focus on the elements of the job/task analysis for which training is needed.
2. Provide clear statements of what is to be learned.
3. Provide the basis for evaluating the participants.
4. Provide the basis for evaluating the effectiveness of the training program.

### B. Lesson plans

1. Lesson plans are required for all training courses conducted or sponsored by the department. It is the responsibility of the individual instructor, whether a member of the department or not, to provide the Chief or his/her designee, with a copy of the lesson plan for approval. A copy of the lesson plan will be maintained along with rosters of personnel attending the training.
2. The lesson plan should include a statement of performance objectives, the content of the training, specification of the appropriate instructional techniques, references, relationship to the job tasks, responsibilities of the participants for the material taught, and plans for evaluation of the participants. The instructional techniques that might be used include the following:
  - a. Conferences (debate, discussion groups, panels, and seminars)
  - b. Field experiences (field trips, interviews, operational experiences, and observations)
  - c. Presentations (lectures, lecture-discussion, lecture-demonstration)
  - d. Problem investigations (committee inquiry, critical incidents)
  - e. Simulations (case study, simulation, games, and role-playing).

### C. Instructors

1. Instructors for all department training programs shall:



- a. Have a minimum of two years law-enforcement experience, or
  - b. Have completed a TCOLE instructor's course and be certified as an instructor, or
  - c. Possess a demonstrated skill in an area of instruction, or
  - d. Have knowledge of teaching theories, methods, and practices along with some knowledge of law-enforcement practices.
2. Instructors enlisted from outside the department shall be approved by the Chief or his/her designee. The instructor must have demonstrated skill in his/her area of instruction and comply with requirements for lesson plans as previously stated. Any compensation will be determined by the Chief of Police.
  3. Before being allowed to instruct any state-mandated courses at the department, instructors shall receive, at a minimum, training in:
    - a. Lesson plan development
    - b. Development of performance objectives
    - c. Instructional techniques
    - d. Learning theory
    - e. Testing and evaluation techniques
    - f. Resources.
  4. Normally, officers selected and trained as instructors in a subject will be expected to teach it when needed for a minimum of two years.

## **VI. REMEDIAL TRAINING**

- A. Remedial training is directed at solving a problem or improving performance in an area within a designated time and with clearly defined, expected results.
- B. Remedial training may be assigned because of discipline or counseling.

## **VII. TRAINING RECORDS (TEXAS BEST PRACTICES: 3.05)**

- A. Training records
  1. The Chief of Police, or his/her designee, shall maintain a training record for each employee that includes the following:
    - a. The date of training

b. The type and hours of training received

c. A copy of any certificate received.

The Texas Commission on Law Enforcement “TCLEDDS” site will be used for sworn members of the department.

Training records for non-sworn members will be maintained separately from those of sworn personnel.

2. The Chief, or designee, shall maintain files on all in-house training courses or presentations, including the following:

a. Course content (lesson plans)

b. Personnel attending

c. Any performance measures as ascertained through tests or demonstrations.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 4.0 Hiring and Selection</b>	
	<b>Effective Date: 06/12/2023</b>	<b>Replaces: November 21, 2021</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
	<b>Reference: TEXAS BEST PRACTICES 2.23, 3.17, 4.01, 4.02, 4.03, and 4.04.</b>	

## I. POLICY

The Teague Police Department strives to obtain the best law-enforcement officers possible to help achieve the department's policing goals. To that end, the department shall practice a regimented, rigorous selection procedure while simultaneously affording equal opportunity to everyone regardless of race, creed, color, sex, national origin, sexual orientation, or age. The department does not discriminate against people with disabilities and affords them the same access to employment provided to all other people. All personnel who participate in screening and hiring applicants shall be guided by fairness, equal opportunity, and consistency in applying the procedures set forth in this order.

## II. PURPOSE

The purpose of this policy is to outline the minimum hiring requirements and the selection process for police officers, cadets, and non-sworn members of the department.

## III. DEFINITIONS

- A. Disability: A physical or mental impairment that substantially limits one or more of the major life activities.
- B. Good moral character: The attributes of a prospective employee that enhance his or her value to the department and the goals of community-oriented policing, among which are honesty, integrity, truthfulness, obedience to the oath of office and the department's code of ethics, respect for authority, and respect for the rights of others.

## IV. QUALIFICATIONS FOR EMPLOYMENT

- A. The minimum qualifications that all applicants for the position of police officer must meet include the following:
  - 1. Age of 21.
  - 2. High school graduation or GED completion.
  - 3. Pass a background investigation that includes the following:
    - a. Personal and family history

- b. Credit history, including current creditors.
  - c. Education, including all schools attended and degrees or certificates obtained.
  - d. All residences for the past ten years
  - e. Comprehensive employment history
  - f. A fingerprint-based criminal history search, including all arrests, locations, dates, and dispositions.
  - g. Traffic summonses and accidents
  - h. An inquiry of family, friends, and associates as to character and reputation, plus an informal interview with the applicant's spouse or "significant other," as well as any ex-spouse.
- 4. Pass an interview.
  - 5. Pass a physical/medical examination, psychological screening, and a drug test.
  - 6. Be of good moral character.

NOTE: Good moral character is determined by a favorable report following the comprehensive background investigation. Also, the interview shall be employed to help evaluate good moral character. Good moral character ensures compatibility with the department's community-oriented policing goals.

- 7. Any other standards set by law or by policy of the Texas Commission on Law Enforcement.

## **V. DISQUALIFIERS FOR EMPLOYMENT**

The following are absolute disqualifiers for employment as a sworn officer:

- A. Conviction or admission of any felony, or a conviction of a Class A misdemeanor.
- B. Conviction of any Class B misdemeanor in the past ten years.
- C. Conviction or admission of marijuana use within the past two years, or of any other illegal drug within the past five years.
- D. Conviction of family violence.
- E. Dishonorable discharge from the military.

## **VI. APPLICATION PROCESS FOR SWORN OFFICERS AND CADETS**

- A. The applicant must do the following:
1. Complete a written city application and a personal history statement and submit them to the Chief of Police.
  2. Submit a copy of each of the following documents:
    - a. Birth certificate
    - b. Driver's license
    - c. High school diploma or transcript, or GED certificate
    - d. Any college transcripts
    - e. Copy of military discharge papers, if any.
  3. Arrange a meeting with the Chief of Police, or his designee, to appear for other steps in the selection process.

**V. SELECTION PROCESS FOR SWORN OFFICERS AND CADETS**  
(TEXAS BEST PRACTICES: 4.01)

- A. The Chief of Police or his/her designee will review the application and documents for basic qualifications. If basic qualifications are met and an opening exists, the Chief may assign a supervisor/officer to conduct a preliminary review of the candidate. If no opening exists, the application will be placed in a file to await an opening for a period of not more than one year. When an opening occurs within 1 year from application submission, the applicant will be contacted to determine if he/she is still interested in the position.
- B. The Teague Police Department has two classifications for Police Officer Applicants, Certified Officer, and Police Cadet. The Department hires qualified Applicants based on Departmental needs and allocation of staffing by the Board of Aldermen. All Applicants must meet the same qualifications and standards. Currently "Certified" competes against "Certified" and "cadet competes against cadet" for ranking on the eligibility list. Upon successful completion of the testing/hiring process, eligible Applicants are placed on an eligibility list effective for 365 days from posting date.
- C. A supervisor/officer may be assigned to conduct a comprehensive background investigation of the applicant. The officer assigned to conduct the background investigation may question the applicant regarding his or her prior medical problems, including any worker's compensation claims and conditions. The officer will then conduct a detailed background investigation in accordance with the Background Investigation Manual. (TEXAS BEST PRACTICES: 4.03)

NOTE: The background check shall specifically include contact with all former law enforcement employers. (TEXAS BEST PRACTICES: 3.17).

- D. The supervisor/officer conducting the background investigation shall have had training in conducting background investigations or shall conduct the background in compliance with the Background Investigation Manual.
- E. The polygraph examination, if used, will be conducted by an operator certified and licensed by the State of Texas to conduct polygraph examinations. (TEXAS BEST PRACTICES: 4.02)
- F. Upon completion of the background investigation, the applicant's file will be returned to the Chief of Police for review, with a recommendation from the background investigator.
  - 1. Any disqualified applicant will be notified, in writing, that they have not been selected for employment.
  - 2. Any qualified applicant will be interviewed by a review board, designated by the Chief of Police. The applicant will be referred to the chief of police with the board's recommendation.
- G. The applicant, if approved by the Chief of Police in consultation with the Board of Aldermen, may be extended a conditional offer of employment.
- H. Applicants given a written conditional offer of employment are scheduled for a psychological examination of the police department's choosing. Those candidates successfully completing the psychological examination are required, at the Police Department's expense, to be evaluated by a Physician of the Police Department's choosing. The Physician will assess each Applicant's physical condition to ensure he/she can perform the essential physical job functions required to be a Teague Police Officer, along with a drug screening. The Teague Police Department is responsible for expenses related to psychological, medical, and drug screening examinations.
- I. Following a psychological, medical, and drug screen examination, an applicant may be withdrawn from the process if the applicant is incapable of performing the core job functions for the position or poses a "direct threat" in the workplace (per EEOC guidelines, "a significant risk of substantial harm to the individual or others that cannot be eliminated or reduced . . . through reasonable accommodation"). The Chief must base the threat on medical knowledge presented to him/her, not just speculation. Any positive results on a drug screen may result in a withdrawal of the conditional offer of employment with the City of Teague.
- J. Unsuccessful applicants who do not have permanent disqualifiers may re-apply after one year from the date of the last application if a vacancy exists.
- K. Successful applicants may be hired at the discretion of the Chief of Police, in consultation with the Board of Aldermen.
- L. Individuals employed in the position of Cadet will be required to enter into a repayment agreement with the City for funds expended by the city for academy and equipment expenses. Cadets will be placed on an 18-month probationary period.

M. Lateral entry.

1. A licensed officer from another Texas agency must meet the same criteria set forth above.
2. The employee assigned to investigate the applicant shall ensure that an applicant with prior law-enforcement experience has not had his or her peace officer license suspended or revoked. A query will be made to the Texas Commission on Law Enforcement to determine all other agencies where the licensee has worked. These agencies will be contacted before completion of the background to determine work history and any significant details of their employment.

**VII. APPLICATION PROCESS FOR NON-SWORN PERSONNEL**

- A. The applicant must do the following for all positions within the police department:
1. Complete a written city application and personal history statement. The completed application and personal history statement must be submitted to the Chief of Police.
  2. Copies of the following documents will also be submitted:
    - a. Birth certificate
    - b. Driver's license
    - c. High school diploma or transcript, or GED certificate
    - d. Any college transcripts
    - e. Copy of military discharge papers, if any.

**VIII. SELECTION PROCESS FOR NON-SWORN PERSONNEL (TEXAS BEST PRACTICES: 4.01)**

- A. The Chief of Police, or designee, will review the application and documents for basic qualifications. If basic qualifications are met and an opening exists, the Chief assigns an officer to conduct a preliminary review of the candidate. If no opening exists, the application will be placed in a file until there is an opening or for one year, whichever is sooner. If an opening occurs within one year, the applicant may be contacted to determine if he/she is still interested in the position.
- B. An employee may be assigned to conduct a comprehensive background investigation of the applicant. The officer assigned to conduct the background investigation may question the applicant regarding his or her prior medical problems, including any worker's compensation claims and conditions. The officer will then conduct a detailed background investigation in accordance with the Background Investigation Manual. (TEXAS BEST PRACTICES: 4.03)

- C. The officer conducting the background investigation shall have had training in conducting background investigations or shall conduct the background in compliance with the Background Investigation Manual. (TEXAS BEST PRACTICES: 3.17)
- D. Upon completion of the background investigation, the applicant's file will be returned to the Chief of Police for review.
  - 1. Any disqualified applicant will be notified, in writing, that they have not been selected for employment.
  - 3. Any qualified applicant will be interviewed by a review board, designated by the Chief of Police. The applicant will be referred to the chief of police with the board's recommendation.
- E. The applicant, if approved by the Chief of Police in consultation with the City Administrator, may be scheduled for a medical, psychological, and drug screening examinations as required.
- F. Following a medical/psychological examination, an applicant may be withdrawn from the process if the applicant is incapable of performing the core job functions for the position or poses a "direct threat" in the workplace (per EEOC guidelines, "a significant risk of substantial harm to the individual or others that cannot be eliminated or reduced . . . through reasonable accommodation"). The Chief must base the threat on medical knowledge presented to him/her, not just speculation.
- G. If the individual is not selected, a letter will be sent to the applicant advising him or her that they have not been selected for employment with Teague Police Department.
- H. Successful applicants may be hired at the discretion of the Chief of Police, in consultation with the City Administrator.


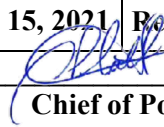
## **IX. PERSONNEL RECORDS**

- A. For each employee, the city maintains a personnel file. This file contains a copy of the background investigation package, a copy of all forms completed during the hiring process, all evaluations, disciplinary action amounting to a written reprimand or higher, leave/attendance record, and assignments. The original of the officer's background investigation and all selection materials are sealed in an envelope, which is confidential, and maintained in a TCOLE ready file. All TCOLE required documents are maintained in a separate file, from the personnel file, and must be secured with access limited to designated personnel. (TEXAS BEST PRACTICES: 2.23, 4.04)
- B. The Chief of Police shall maintain and control all TCOLE required personnel records. The City Secretary is the custodian of record for the city and maintains all personnel files. The department complies with the records retention schedule set by state law and city policy. (TEXAS BEST PRACTICES: 4.04)
- C. Employees may review their records at any reasonable time upon request. The Chief may release a copy of a record from the file upon obtaining a signed authorization from the employee or in conjunction with an appropriate submitted open records request.



- D. All personnel records are considered confidential. Supervisory or investigative personnel who have a need to review sensitive information may do so only with the express approval of the City Administrator or Chief of Police.
- E. If the Chief deems it necessary to include derogatory information in a personnel file, he/she shall notify the employee of the fact in writing. The employee may protest the inclusion of such information in writing to the Chief.
- F. Personnel records are the permanent property of the City of Teague.
- G. Officers from the department may terminate their employment and seek a lateral hire with another agency. Requests for employment information on these officers shall be referred to the Chief. The Chief shall disclose the employee's performance record consistent with current law, when requested, and a properly executed release form is obtained from the subject of the records in compliance with Texas Occupations Code 1701.451 and TCOLE Rules.
- H. All records of unsuccessful applicants shall be maintained, including all test results (if any), in a confidential file by the Chief of Police. These records can be released to other law enforcement agencies when requested and a properly executed release form is obtained from the subject of the records. (TEXAS BEST PRACTICES: 4.04)
- I. Photographs of sworn officers shall not be released by the department to any organization or media outlet, nor shall any be posted on any department website, or in a publicly displayed department yearbook or photograph unless the officer has given his or her consent or signed a release to that effect. Exceptions to this prohibition include:
  - 1. If the officer is charged by indictment or information.
  - 2. If the officer is a party in an arbitration process.
  - 3. If the officer's photograph is introduced in judicial proceedings.

NOTE: Photographs displayed on officer's identification cards are not considered released as they are intended for internal use or to properly identify an officer if required.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 4.1 Appointment and Probation</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: TEXAS BEST PRACTICS 1.09 and 2.03</b>	

## I. POLICY

The Teague Police Department is committed to ensuring that the standards of the department are maintained and that the people of our city are served by a competent and professional police department.

## II. PURPOSE

The purpose of this policy is to provide a systematic process for the appointment of sworn and non-sworn personnel.

## III. PROCEDURES FOR SWORN PERSONNEL

- A. Applicants who have been through the hiring process and have been approved for hire, by the Chief of Police in consultation with the City Administrator, will complete the following steps prior to being retained as full-time police officers:
  1. The applicant will meet with the Chief of Police, or designee, and determine a starting date.
  2. On the day selected for employment, the applicant will report to the city personnel office for completion of all initial paperwork. Issuance of an identification card will be done by the Chief of Police.
- B. Upon completion of the initial processing, the new employee will report to the police department where he/she will be issued the appropriate equipment. The employee shall sign for the issued equipment.
- C. The new employee shall be issued a complete and up-to-date copy of the department's policies, SOPs, and field manuals.
- D. The Chief, or designee, shall set a time and place where the new officer shall swear the oath of office before a public gathering. The new officer must take and sign the oath of office before performing any law enforcement duties. (TEXAS BEST PRACTICES: 2.03)
- E. The Chief, or designee, shall also assign the new employee to a senior training officer for initial field training. The new employee will work the same hours and days off as the field-training officer.

- F. The new officer must possess a valid Texas peace officer license before performing any law enforcement functions. If the officer begins work before attending a basic academy and obtaining a license, he or she shall perform non-police duties only and shall accompany experienced officers as an observer only. (TEXAS BEST PRACTICES: 1.09)


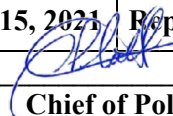
#### **IV. PROCEDURES FOR NON-SWORN PERSONNEL**

- A. Applicants who have been through the hiring process and have been approved for hire will complete the following steps prior to being retained as full-time employees:
  - 1. The applicant will meet with the Chief of Police and determine a starting date.
  - 2. On the day selected for employment, the applicant will report to the city personnel office for completion of all initial paperwork. The chief of Police shall issue an identification card.
- B. Upon completion of the initial processing, the new employee will report to the police department where he/she will be issued any necessary equipment for a job assignment. The employee shall sign for any issued equipment.
- C. The new employee shall be issued a complete and up-to-date copy of the department's policies, SOPs, and field manuals
- D. The employee will be assigned to another employee, if necessary, for training as required and shall receive training in department operations, personnel rules, and departmental philosophy.

#### **V. PROBATION**

- A. All new employees are on probation for a period of six months, in accordance with city policy.
- B. An employee may be released from employment at any time during the probationary period for any reason. Supervisors who believe a probationary employee's job performance is unsatisfactory should provide evidence of the unsatisfactory performance to the Chief of Police for consideration at any time.
- C. A new employee's supervisor shall rate the new employee using the employee evaluation form on monthly anniversary dates from employment for non-sworn employees. Sworn officers will be rated as required by the field-training manual. Two weeks prior to the six-month anniversary, the supervisor shall complete and forward a final evaluation form to the Chief of Police recommending the employee be retained or terminated. If the recommendation is for termination, the supervisor shall document the specific work-related performance that is deficient. The work performance of each probationary employee shall be evaluated using valid, non-discriminatory procedures.

- D. Prior to the end of the probationary period, the Chief of Police shall review the performance evaluation. The Chief may approve the employee's permanent appointment or recommend discharge of him/her, for failure of probation, to the City Administrator.
- E. The employee, after consultation with the City Administrator, may be dismissed from employment for unsatisfactory performance of their essential duties by the Chief of Police.
- F. Probationary employees who wish to protest their performance may do so in accordance with city policies.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 4.2 Career Development, Promotions, and Transfers</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 4.06 and 4.07	

## I. POLICY

The department encourages employees to seek opportunities to develop their knowledge, skills, and abilities. Promotions are based on performance, longevity, and the growth of skills through training and experience. Although in small department as such as ours, promotional opportunities are rare, the department promotion process is fair and equitable

## II. PURPOSE

The purpose of this policy is to establish guidelines for career development of employees, which includes training and promotions.

## III. PROCEDURES

### A. Responsibilities of the Chief of Police

1. Annually, the Chief of Police, or designee, will meet with each employee for career counseling. This counseling shall occur at the same time as the employee's annual performance evaluation. The counseling shall include an examination of the following:
  - a. The employee's performance record
  - b. A review of the training programs applicable to the employee's duties.
2. The Chief shall ensure that at least one department employee:
  - a. Achieves and maintains certification as a firearms instructor
  - b. Receives advanced instruction in the techniques of evidence collection.
3. All officers shall maintain current first aid/cardiopulmonary resuscitation certifications.
4. The Chief shall ensure the availability of a trained armorer, either through the training of a department employee, contracting with an armorer in another jurisdiction, or contracting with a private armorer. The armorer shall inspect all firearms and ammunition at least annually for safety, reliability, and function. The armorer shall also repair broken or malfunctioning weapons.

5. The Chief of Police shall ensure that any employee who receives a promotion or a new assignment receives training specific to that position within 12 months of assignment.

B. Promotions (TEXAS BEST PRACTICES: 4.06)

When a vacancy exists for the position of sergeant the Chief shall post an advertisement of the position, the qualifications required, and a description of the selection process to be used. This advertisement must run for a minimum of two weeks prior to any selection process. During that time, officers may request, in writing, consideration for the position.

C. Eligibility for Promotion. An employee must meet the minimum requirements as listed below to be eligible for promotion to a higher level of responsibility and increased compensation:

1. Sergeant: To compete for sergeant, a candidate must have a minimum of four years police experience, as a police officer, and at least one-year time in the next lower position with this agency. The candidate must have, at the very least, Intermediate Peace Officer Certification issued by the Texas Commission on Law Enforcement.
2. All candidates: Their overall performance evaluation score must be at least satisfactory for the 12 months prior to the promotional examination process.
3. Each candidate must submit a "letter of intent" to the office of the Chief of Police that requests participation and consideration in the promotional selection process.
4. The Chief of Police may go outside the department to fill ranking positions if circumstances dictate.


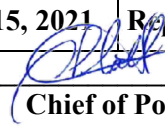
D. Process for Promotions.

1. Sergeant
  - a. Meet eligibility
  - b. Submit "letter of intent"
  - c. Review by Chief of Police
    - i. The "rule of three" shall apply. As promotions become available, the top three names will be sent to the Chief for consideration. The Chief shall promote candidates in order unless there is justification to pass over a candidate.
    - ii. The Chief of Police may pass over any person on the list if there is a compelling reason to do so, such as poor evaluations or disciplinary reasons.
  - d. Candidates selected by the chief for promotion will be submitted to the Board of Aldermen for approval of the promotion.

- e. The eligibility list will be valid for one year from the date of the publication.  
(TEXAS BEST PRACTICES: 4.07)
- f. Promotional Probation. The Chief of Police will announce promotions and the effective dates. All promotions are conditional in that the employee must satisfactorily complete a six-month probation period.

#### E. Transfers

- 1. The Chief may assign or transfer any employee to a different duty when he/she deems that such action will be in the best interests of the department.
- 2. Any employee may request a transfer by writing a memorandum to the Chief.
- 3. Occasionally, some job assignments require minimum assignment periods so that the department may sufficiently benefit from investments in specialized training or education. Minimum periods of assignment shall be determined by the Chief and specified in a departmental order. The Chief reserves the right to establish minimum and maximum terms of service for selected duty assignments when he/she deems it to be in the best interest of the department.
- 4. Officers engaged in undercover assignments are subject to rotation after a period of one year, although they may continue to perform investigative work.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 4.3 Performance Evaluations</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: 4.08 and 4.09</b>	

## I. POLICY

The department bears an obligation to the public and its own personnel to hire and retain the best qualified officers. Further, the department's community-oriented policing philosophy demands that officers exhibit not only competent investigative skills but also that they succeed in communicating with many different individuals in a variety of contexts. To that end, the department regularly and formally evaluates the performance of officers and other employees. The evaluation system discussed herein serves both the interests of management and employees. The purposes of the evaluation system are to (1) ensure fair and impartial personnel decisions, (2) maintain and improve performance, (3) provide a basis and a medium for personnel counseling, (4) assist decisions about the tenure of probationary employees, and (5) identify training needs.

## II. PURPOSE

The purpose of this policy is to outline and describe the departmental evaluation process.

## III. PROCEDURES

### A. General


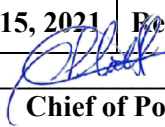
1. All employees shall be evaluated using the Board of Aldermen approved form.
2. Supervisors will be trained in the evaluation process prior to conducting the evaluations. (TEXAS BEST PRACTICES: 4.08, 4.09)
3. Personnel shall be rated as having demonstrated unacceptable, acceptable, or superior behavior. The rating reflects the observations and perceptions of rating personnel.
4. After completion of probation, each officer shall be evaluated on their annual anniversary. Employees who fail to receive an overall satisfactory evaluation rating may be placed on probation for a period determined by the Chief of Police or City Administrator. Within the probation period, the employee shall receive remedial training in deficient areas, and demonstrate proficiency (or satisfactory improvement) in deficient areas. The training and improved behavior will be documented on the evaluation form.



5. Except for probationary employees, all performance evaluations will cover one calendar year and shall be completed, signed by the employee and the rating supervisor, and turned in to the Chief of Police before the anniversary date of hire for the evaluated employee.
6. All evaluations shall be reviewed with the employee and placed in the employee's personnel file.
7. All newly hired employees and officers in their probationary period shall receive monthly written evaluations if no significant deficiencies are observed.
8. Officers shall be evaluated informally by their immediate supervisor. A formal evaluation is conducted by the Chief of Police, in accordance with city policy.
9. An officer who receives an unsatisfactory rating which he or she perceives to be unjust may appeal to the next level of the chain of command up to the City Administrator. The officer concerned must rebut the comments or rating in writing and submit the rebuttal through the chain of command.

B. Evaluation of non-sworn employees and supervisors

1. Non-sworn employees shall be evaluated on forms approved by the Board of Aldermen.
2. Supervisors shall be evaluated by their next level supervisor. Under "comments" the rater shall refer to an attached page that will contain, in narrative form, comments concerning the individual's supervisory performance. The rater shall address, at a minimum, the following points:
  - a. Ability to instill in officers a high regard and respect for community-oriented policing ideals, the rule of law, civil rights, and concern for victims.
  - b. Ability to perceive performance weaknesses in his or her officers, conduct remedial training, and document improved proficiency.
  - c. Command of patrol techniques, methods, and investigative procedures.
  - d. Ability to reprimand, counsel, praise, or otherwise discipline his or her officers.
  - e. Ability to take responsibility for the performance of his or her officers.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 4.4 Uniforms, Appearance, and Equipment</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 1.11, 1.12, 2.13, 7.17, and 7.23.	

## I. POLICY

Proper uniforms and equipment are essential to the performance of our law enforcement duties. Officers must present a professional image to the community we serve, one that promotes respect and confidence. All employees must strive to present a clean, well-groomed image when wearing the departmental uniform or representing the department in any capacity.

## II. PURPOSE

The purposes of this policy are to provide officers with a list of uniform and equipment items and to provide a departmental dress code for all employees, sworn and unsworn.

## III. UNIFORMS AND EQUIPMENT

- A. New employees shall be issued the uniforms and the equipment needed to perform their duties. Employees may purchase and carry additional items that are approved and authorized in writing by the Chief of Police. Employees will not wear, carry, or use any personally owned equipment without the written approval of the Chief of Police, a copy of which will be kept in the employee's departmental file. (TEXAS BEST PRACTICES: 1.11)
- B. Each employee must sign an inventory sheet listing all uniform and equipment items issued to the employee. The inventory sheet will be maintained in the employee's departmental file.
- C. Employees are responsible for the uniforms and equipment issued.
- D. The employee's supervisor shall ensure that all departmental uniforms and equipment are returned to the department upon resignation, termination, or retirement. Failure to return all items of city property may result in legal action against the employee. (TEXAS BEST PRACTICES:1.12)
- E. Employees shall have as a part of their issued equipment a copy of the rules and regulations and a copy of the policy manual. Employees shall maintain these and make appropriate changes or inserts as directed.

#### **IV. UNIFORMS AND EQUIPMENT PROVIDED BY THE CITY**

- A. Uniforms and equipment provided to police officers by the City of Teague shall include:
1. Three (3) pair of trousers
  2. Two (2) short-sleeved shirts
  3. Two (2) long-sleeved shirts
  4. One (1) tie
  5. One (1) shirt badge
  6. One (1) name plate
  7. One (1) raincoat
  8. One (1) winter jacket
  9. One (1) set of leather/nylon gear which includes belt, holster, handcuff case, magazine case, and radio case
  10. One (1) protective vest (body armor)
  11. One (1) traffic vest
  12. One (1) baton and baton holster
  13. One (2) set handcuffs
  14. One (1) duty handgun and magazines
  15. One (1) patrol rifle and magazine
  16. Rank insignia as needed
- B. Uniforms and equipment that are excessively worn or damaged are replaced by the department. An employee requesting replacement should have the item inspected by his/her supervisor, who will forward a written request for the replacement to the Chief of Police.
- C. With the written approval of the Chief of Police officers can purchase additional uniforms and equipment as needed or desired. These items may be purchased from any vendor, but they must comply with current uniform or equipment standards.
- D. Replacement of personally owned uniforms, equipment, or jewelry -- including watches -- that are lost or damaged in the performance of duty shall be the responsibility of the employee.
- E. Uniform items and equipment meeting departmental specifications and provided by individual officers shall include the following:
1. Black, white, or Navy-blue undershirts
  2. Black or Navy-blue socks
  3. Footwear, black leather
- F. Civilian business attire (coat and tie for men or equivalent for women) shall be worn for all court appearances if the employee is a civilian or in a plain clothes assignment. Officers shall wear their issued class "A" uniform, consisting of long sleeve shirt and necktie for all court appearances.

## **V. PROTECTIVE VESTS (TEXAS BEST PRACTICES: 7.23)**

- A. Body armor is purchased by the department for all sworn officers. Body armor will be replaced in accordance with guidelines and protocols established by the National Institute of Justice.
- B. Uniformed Officers, when working field assignments, will wear departmentally issued protective vests when on-duty or when off-duty if they are engaged in law enforcement activities. Officers not working field assignments will maintain their vests where they are readily accessible in the event they are needed. Any officer participating in any search warrant execution or other high-risk activity SHALL wear a protective vest.
- C. The Chief of Police may grant exceptions to this requirement during periods of extreme weather. During such periods, officers working in the field must keep their protective vests where there are immediately accessible.
- D. Officers shall routinely inspect personal body armor for signs of damage and for general cleanliness. Because dirt and perspiration may erode ballistic panels, each officer shall be responsible for cleaning personal body armor in accordance with the manufacturer's instructions.

## **VI. REFLECTIVE VESTS**

Agency personnel are issued and shall wear the high-visibility reflective vest as soon as practical when directing traffic or working at the scene of an accident. (TEXAS BEST PRACTICES: 7.17)

## **VII. DEPARTMENTAL APPEARANCE REQUIREMENTS (TEXAS BEST PRACTICES: 2.13)**

- A. Uniform Employees
  - 1. When wearing the uniform, employees will be in full uniform, including all items that are integral parts of the uniform. All uniform and accessories must be clean and well pressed. No part of the uniform is worn with civilian clothing or vice-versa.
  - 2. Undershirts worn with an open-collar, short-sleeve shirt shall be blue, white, or black in color. Shirrtails will always be worn tucked in. Employees wearing a long-sleeved shirt may wear a dark navy or black turtleneck or mock turtleneck during cold weather.
  - 3. Rank Insignia. The Chief will wear a single gold star on each point of the uniform shirt collar. Employees holding the rank of sergeant will wear embroidered chevrons approximately  $\frac{1}{4}$  inch below the department-issued shoulder patch with the single point up.

4. Nameplates and name tabs. Uniforms worn for regular duties will have a name tab sewn on the shirt, in line with the top edge of the right pocket. The name tab will be blue background for all officers. For officers holding the rank of sergeant or higher will be gold thread (for the name only) and those with a rank below sergeant will be silver thread.
5. Each employee, regardless of rank, will wear a departmentally issued nameplate (metal), on their class "A" centered above the right shirt pocket and in line with the seam. The nameplate will have the officer's first initial or first name and last name. The nameplate for officers holding the rank of sergeant or higher will be gold while those with a rank below sergeant will be silver.
6. Department Shirt Badges. All sworn personnel when in the standard duty uniform will wear their department badge prominently displayed above the left-shirt pocket. The uniform utilized for regular duty will have a sewn-on badge. The metal badge is worn with the class "A" or dress uniform.
7. Footwear. Footwear will be solid black and capable of being shined. Officers must wear solid navy blue or black socks if the socks are visible.
8. Officers are authorized to wear baseball style caps only during inclement weather or in conjunction with a utility uniform during specialized assignments or outdoor training. Winter headgear may consist of a navy blue or black knit cap with no visible logos or emblems.

#### B. Award Ribbons or Medals

Commendation ribbons and medals approved for wear by the department may be worn, centered, above the nameplate on the uniform shirt, no more than three across and three up, and will be worn in order of importance. The wearing of commendation ribbons and medals is optional for those officers who are recipients of such awards while wearing the standard duty uniform and while assigned to standard duty assignments. The wearing of commendation ribbons and medals is mandatory for those officers who are recipients of such awards in all formal settings (class "A" or dress uniforms).

#### C. Plain Clothes Assignments (Sworn and Non-Sworn Employees)

Except for officers working in a covert capacity, clothing worn by employees in any departmental, non-uniform assignment will conform to accepted business practices. These include but are not limited to the following:

1. Slacks, dress shirts (long or short sleeved), ties (excluding bow ties), socks, shoes, and appropriate headwear.
2. Headwear must be appropriate for business dress attire, and the item must have prior approval from the Chief or his/her designee.
3. Business or sports coats are optional unless required for a court appearance or other specific event or task.

4. Socks should coordinate with the pants. White socks are prohibited unless worn with boots that conceal the socks.
5. Footwear should be clean and polished, with heels and toes in good repair. Normal business shoes, including slip-ons (loafers) or lace-ups, are acceptable. Boots are acceptable, provided they are in good taste. Flip-flops and sandals are inappropriate.
6. Female business attire will include the previously mentioned clothing and non-revealing blouses, skirts, dresses, and appropriate footwear. Flip-flops and sandals are inappropriate.
7. If a sidearm is worn on the waist, the officer's department badge must be prominently displayed next to the sidearm.
8. Plain-clothes officers may wear a vest or jacket that readily identifies the wearer as a police officer during callouts, specific assignments, or extra-duty assignments when appropriate.
9. Plain-clothes sworn personnel are always required to maintain at least one complete standard uniform in case they are called upon for uniformed duties.

#### D. Special Assignments

Employees placed in special assignments, including covert or undercover assignments, special events, or other special operations, will wear clothing approved by the Chief of Police or the supervisor of the operation.

#### E. Court Attire

Officers attending court will be in class "A" uniform or civilian business attire for male employees and appropriate business attire for female non-sworn employees.

#### F. Physical Appearance

1. Employees shall maintain their physical appearance in accordance with good taste and professionalism. Hair shall not be dyed, colored, or styled in a manner that would draw undue attention to the employee. Female employees will apply their makeup tastefully. Male employees shall not appear for work needing a shave or haircut.
2. Hair length
  - a. Male employees shall wear their hair to present a groomed appearance. Hair will not extend past the collar at the back of the neck. Hair on the sides will not extend below the top of the ear and must be mildly tapered. Hair in the front will not extend below the middle of the forehead.

- b. Female employees shall wear their hair to present a groomed appearance. They shall not be restricted as to the length of their hair; however, if the hair extends below the bottom of the collar it shall be secured in a bun or ponytail. It shall not hang into the employee's face, either in front or on the sides.
3. Sideburns, Mustaches, and Beards
    - a. Sideburns - Sideburns shall not exceed beyond a point even with the bottom of the ear lobe and shall extend in a clean-shaven, horizontal line. The flare (terminal portion of the sideburn) shall not exceed the width of the main portion of the sideburn by more than one-fourth of the unflared width. The sideburn shall be trimmed and neat in appearance.
    - b. Mustaches - A mustache of natural color may be worn. Mustaches shall not exceed below the vermilion border of the upper lip and may not extend to the side more than one-half inch beyond the corners of the mouth. No mustache shall be waxed, twisted at the ends, and/or pulled to a point.
    - c. Beards - Employees may wear a close-cropped beard or goatee with the understanding that said beard or goatee must not be of a length that would allow anyone to grab and pull said beard or goatee and/or use the beard or goatee as a method of attacking or gaining control of an officer. The beard or goatee must always be kept neat.
    - d. Revocation of an employee's right to wear a Sideburns, Mustaches, Beards or Goatees is at the discretion of the Chief of Police. Revocation may occur if in the Chief's opinion, the beard is not neat and/or close cropped.
4. Jewelry
    - a. Female employees may wear earrings, provided they are small and tasteful in appearance. Male employees are not permitted to wear any type of earring.
    - b. Employees in uniform are discouraged from wearing chains and necklaces as they could be lost or cause an injury during the performance of police activities. If worn, they should be concealed behind their undershirt.
    - c. A female employee in civilian attire may deviate from these regulations with the approval of her supervisor.
    - d. To present a uniform and objectively neutral appearance to the public, non-departmental jewelry or pins shall not be worn on the uniform at any time or on plain clothes while on duty unless specifically authorized by the Chief of Police.

## 5. Personal Hygiene

Employees shall always practice good personal hygiene, including use of soap, water, and deodorant. Employees shall not report for work emitting an offensive body odor. A moderate amount of perfume or aftershave may be used.

## 6. Tattoos, Body Art, Piercing, or Branding

a. Tattoos or brands that are prejudicial to good order are prohibited. Additionally, while on or off duty in uniform or on duty in civilian attire, employees are prohibited from exhibiting tattoos, body art, or brands that are offensive or demeaning to persons of ordinary sensibilities. This policy may be rescinded or modified at any time by the chief of police.

### b. Definitions

- i. Body modification: a deliberate altering of the human anatomy or human physical appearance
- ii. Brand: a picture, design, or other marking that is burned into the skin or other areas of the body. Body markings are pictures, designs, or other markings using means other than burning to permanently scar or mark the skin.
- iii. Extremist: extremist tattoos or brands are those affiliated with, depicting, or symbolizing extremist philosophies, organizations, or activities. Extremist philosophies, organizations, and activities are those which advocate hatred or intolerance based on race, ethnicity, national origin, gender, sexual orientation, gender identity, religion, economic status, age or disability; advocate create, or engage in illegal discrimination based on race, ethnicity, national origin, gender, sexual orientation, gender identity, religion, economic status, age or disability; or advocate violence or other unlawful means of depriving individual rights under the U.S. Constitution, and Federal or State law.
- iv. Indecent: indecent tattoos or brands are those that depict nudity or are offensive to modesty, decency, propriety, or professionalism.
- v. Political: relating to the symbols, causes, ideas or strategies of a party or group in politics, including special interest groups
- vi. Racist: racist tattoos or brands are those that advocate a philosophy that degrades or demeans a person or group of people based on race, ethnicity, or national origin.
- vii. Sexist: sexist tattoos or brands are those that advocate a philosophy that degrades or demeans a person or group of people based on gender.



- viii. Tattoo/body art: defined as a picture, design, or marking made on the skin or other areas of the body by staining it with an indelible dye, or by any other method including pictures designs or markings only detectible or visible under certain conditions (as in an ultraviolet light or invisible ink tattoo). The term tattoo and body art are interchangeable.
- c. The following tattoos, body art, and brands are prejudicial to good order and are prohibited for all employees, regardless of visibility:
  - i. Extremist
  - ii. Indecent
  - iii. Sexist
  - iv. Racist
- d. Officers are prohibited from having tattoos on any part of the hands, neck, face, head, eyelids, mouth, and ears with the following exceptions:
  - i. Tattoo of one wedding band on a ring finger.
  - ii. Permanent facial make-up on the eyebrows, eyeliner, and lips that is conservative.
- e. Any tattoo/body art or brand that implies a negative bias toward any group will cause the employee to be subject to disciplinary action, up to and including termination.
- f. The department reserves the right to require employees to conceal their tattoos/body art or brands if deemed necessary to comport with evolving community standards, attitudes, or beliefs. This policy and its exceptions do not grant permanent approval to display any tattoos/body art or brands subsequently deemed unacceptable for display and employees may be required to cover them at any time.
- g. The following tattoos/body art and brands must be concealed in accordance with this policy while in uniform, on or off duty or on duty in civilian attire:
  - i. Symbols or markings likely to elicit a strong negative reaction in the workplace or public or that are inconsistent with the department's values or community relations objectives, including but not limited to symbols or markings that promote or are associated with violence or weaponry.
  - ii. Anything contrary to the purpose of law enforcement, including, but not limited to: depictions symbolizing or indicative of alcohol or narcotics, illegal or gang related activity, or symbols suggestive of activity that undermines the purpose of law enforcement.

- iii. Illustrations, references, symbols, acronyms or the like that denigrate the United States, State of Texas, or the Teague Police Department.
- iv. Symbols or markings that represent political beliefs, political parties, political slogans, or that cast any political group in a negative light.
- h. Sworn and uniformed civilian employees may have pierced ears, but body piercing of the face, head, neck, nose, mouth, and hands is prohibited. For all employees, piercing or alteration to any area of the body visible in any authorized uniform or civilian attire that is distracting, inconsistent with a professional appearance or noticeably distorts normal anatomical features and that is not medically required, nor a reasonable elective cosmetic surgery performed by a licensed physician, is prohibited. Such prohibited body alterations include, but are not limited to:
  - i. Tongue splitting or bifurcation.
  - ii. Complete or transdermal implantation of any objects other than hair replacement or other reasonable elective cosmetic surgery performed by a licensed physician.
  - iii. Abnormal shaping of the ears, eyes, or nose.
  - iv. Outlandish or unnatural contact lens colors or color variations that detract from a professional appearance.
  - v. Gauging or gradually increasing the radius of a surgically induced opening in the flesh in areas such as the earlobes or lips.
  - vi. Abnormal filing or filling of the teeth.
  - vii. Dental jewelry or unnatural appearing covers such as "grills."
  - viii. Extraocular implants.
  - i. Procedures medically necessary because of illness, deformity, or injury and performed by a licensed physician shall not be considered body modifications for the purpose of this policy.
  - j. Tattoos that must be concealed under this policy must be kept entirely from view by the authorized uniform or plainclothes when an employee represents the department on duty or off duty.
  - k. If when considering a new tattoo, an employee should submit the design to the Chief of Police for approval.
  - l. Any tattoo/body art that is believed to not conform to this policy should be brought to the attention of a supervisor. The supervisor will notify the Chief of Police.


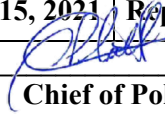
- m. The chief of police shall make the final determination as to whether tattoos/body art conform to this policy.
- n. Prospective employees
  - i. Employment packages will include the information on all tattoos/body art of the applicant to ensure the applicant does not have any tattoos/body art that is prohibited by this policy.
  - ii. The Administrative Services Bureau Chief or chief of police will make the final determination as to whether an applicant's tattoos/body art comply with this policy.

#### **VIII. USE OF DEPARTMENTAL FACILITIES AND EQUIPMENT AND EXPECTATION OF PRIVACY.**

All employees, reserves, and volunteers are advised that the use of departmental facilities, lockers, vehicles, and any equipment, including computers, telephones, or other electronic devices, is governed by departmental rules and regulations and that there is no expectation of privacy regardless of whether locks, passwords, or privacy settings are employed.

No equipment or supplies belonging to the City may be used by employees for supplemental/outside employment.

On or before the last day of employment with the City, all departing employees must return all equipment, supplies, files, and resources provided to the employee by the City during the employee's tenure with the City.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 4.5 Off-Duty Employment</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 4.05</b>	

**I. POLICY**

The Chief of Police must ensure the continued efficiency and effectiveness of the department while simultaneously reducing or eliminating conflicts of interest. To promote the welfare and good reputation of the department this order outlines procedures to ensure appropriate, accountable, and reasonable off-duty work.

**II. PURPOSE**

The purpose of this policy is to define regulations governing off-duty employment and conduct for an officer who is employed in an off-duty capacity.

**III. DEFINITIONS**

- A. Off-Duty Employment: Work not done as part of regular employment by this department, but which is performed, or which provides services for compensation (a fee or otherwise), including self-employment. Volunteer charity work is excluded unless it involves law-enforcement duties.
- B. Employment related to law enforcement: Off-duty employment that may entail the use of law-enforcement powers granted by the State of Texas or the City of Teague.
- C. Probationary period: The period measured by one calendar month beginning with the date of hire.
- D. Secondary employment: Any off-duty work for pay that is not related to law enforcement. Secondary employment that does not require sworn enforcement powers as a condition of employment and the work does not provide implied law-enforcement service.

**IV. PROCEDURES (TEXAS BEST PRACTICES: 4.05)**

- A. General.
  - 1. All employees are eligible to work off-duty employment subject to the requirements of this policy and of the city policy.
  - 2. No employee shall work off duty employment during their probationary period.

3. Employees on medical, sick leave, temporary disability, light duty, unpaid leave of absence for personal reasons, worker's compensation leave, or other types of absenteeism from primary duties are ineligible for off-duty employment.
  4. The obligation to the City of Teague is the primary obligation of any employee. An employee engaged in any off-duty employment may be called to duty in an emergency without regard to their off-duty employer's requirements.
  5. An employee will not be covered by the City's workers' compensation insurance while working for another employer or while self-employed unless the employee is required to perform official City employment activities while engaged in such outside or self-employment.
- a. Secondary employment restrictions: conflict of interest.

Employment shall not in and of itself constitute a conflict of interest. A conflict of interest, as determined by the Chief of Police, is any activity that is inconsistent, incompatible, or in conflict with the duties, functions, or responsibilities of police department employment.


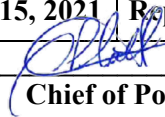
- b. Restriction on off-duty employment that is law-enforcement related.
- i. Employment related to law enforcement shall not exceed 16 hours per day, including on-duty time. For example, an employee working a 10-hour tour may work six hours of off-duty employment on the same day, and an officer on a day off may work 16 hours. For computing allowable work time, court appearances or other duty related functions constitute on-duty time.
  - ii. Officers will not work any off-duty employment on the same calendar day they call in sick to on-duty employment, are on administrative leave, or are suspended due to disciplinary matters.
  - iii. Employment related to law enforcement is restricted to the city boundaries and only on the approval of the Chief of Police.
  - iv. The minimum salary required for officers employed in a law-enforcement related capacity may be determined by the Chief of Police for similar types of employment.
  - v. Serving as a recruiter and receiving compensation for procurement of law-enforcement related jobs for other department employees is prohibited.
  - vi. No employee shall solicit any person or business for the purpose of gaining law-enforcement related off-duty employment, and, while on duty, shall not solicit any person or business for the purpose of gaining secondary employment.
  - vii. City-owned vehicles, radios, badge, police identification, or other equipment shall not be used while engaging in law-enforcement related off-duty employment. This includes the use of city-owned vehicles to commute to and from off-duty related employment.

- viii. Officers engaged in law-enforcement related employment shall be subject to the orders of the on-duty law-enforcement supervisor.
  - ix. Officers shall adhere to all city and departmental policies while engaged in off-duty related employment.
  - x. Employees may not accept outside or self-employment that conflicts with the effective performance of the employee while on duty with the City, or conflict in any way with the best interests of the City. Other outside activities, such as volunteer activities, that might similarly distract from an employee's ability to perform his or her job with the City are also prohibited.
  - xi. No employee shall work any outside employment without the approval of the Chief of Police.
  - xii. The Chief of Police may, at his/her discretion, revoke any officers privilege for working outside employment, to include law enforcement related work.
- c. Administration.
- i. Employees must annually submit a written request to the Chief of Police through the chain of command for any off-duty employment. Employees shall not begin any off-duty work until approval has been granted. The request shall be filed in the employee's personnel file.
    - 1. The approved request is subject to periodic review by the Chief of Police. Officers shall communicate any changes in information contained on the form to the Chief of Police as soon as possible.
    - 2. The Chief of Police may revoke permission to work off duty if the officer fails to perform adequately on duty or receives disciplinary action. To be eligible for permission to work off duty, officers must be in good standing with the department. Continued permission to work off duty is contingent upon remaining in good standing.
  - ii. The Chief of Police shall disapprove any employment that demeans the status or dignity of the law-enforcement profession or otherwise represents a conflict of interest. Examples of such employment include the following:
    - 1. Retailers that sell pornographic materials or provide services of a sexual nature.
    - 2. Retailers who sell, manufacture, or transport alcoholic beverages as the principal business.
    - 3. Gambling establishments not exempted by law.
    - 4. Any firm connected with the towing or storage of vehicles, bill collecting, bodyguards, re-possessors, private investigators, or process servers.

5. Performance in department uniform of any tasks other than those of law enforcement.
  6. Performance of any work for a business or labor group that is on strike.
  7. Performance of any work regulated or licensed through the department.
  8. Performance of personnel investigations for private firms, or any employment requiring the officer to have access to police files, records, or information as a condition of employment.
  9. Performance of any activity that supports case preparation for the defense in any criminal or civil action.
  10. Performance of controversial or political protests of any kind.
- iii. Arrests made while engaged in off-duty law-enforcement related employment shall be limited to felonies or criminal misdemeanors committed in the officer's presence or a breach of the peace jeopardizing public safety.
  - iv. Employees shall understand that department liability protection does not extend to willful acts that cause injury or damage, or acts the officer knew or reasonably should have known conflicted with department policy or the law.
  - v. Off-duty arrests shall not be made when the officer's actions only further the interests of the private employer.
  - vi. Officers will not enforce by arrest, request, or threat any house rules or private employer rules.
  - vii. Officers shall contact the on-duty officer/supervisor, or agency having jurisdiction, to handle any criminal case they encounter in an off-duty capacity.
  - viii. Violations of this policy may constitute grounds for disciplinary action.
- d. Liability, indemnification, insurance
- i. All employees who wish permission to engage in law-enforcement related employment shall complete the application for outside employment. The Chief of Police must grant permission before the employee may work off duty. In addition to the application form, the employee must submit to the Chief of Police a copy of the contract with the off-duty employer. The contract must specify the following:
    1. The precise nature of the work to be performed.
    2. Hours or schedule of the work to be performed.

3. What equipment the employee must maintain.
  4. Insurance coverage of the business providing for medical treatment for job-related injuries and indemnification for litigation arising from off-duty employment.
- ii. The department shall not be responsible for medical expenses incurred from injuries sustained while working in any off-duty employment.
  - iii. The department recognizes that an officer in law-enforcement related employment may undertake an action connected with the employment that the courts may construe as a law-enforcement duty, and, therefore, an extension of the job. Officers are reminded that their off-duty performance must meet the same standards required for on-duty performance. Off-duty law-enforcement actions, whether for a private employer or not, must meet the requirements of this manual.
  - iv. Court cases resulting from off-duty employment are not compensated by the department or city, for remuneration of salary for such required services of the officer involved. Any remuneration required due to court appearances, relating from off-duty incidents, shall be the responsibility of the off-duty employer.
- e. Dual Commissions
- i. No officer of this department is authorized to be commissioned by another law enforcement agency, while employed as a commissioned officer with Teague Police Department.



	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 4.6 Grievance Procedure</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 2.08</b>	

## I. POLICY

The department's goal is to provide fair, equitable, and clearly defined means for the resolution of grievances, to ensure that employees and their supervisors are accorded reasonable opportunity to present the facts bearing on a grievance, and to guarantee the opportunity to exercise the rights set forth in this order. Every employee has the right to fair treatment in all matters arising from employment and to this end each employee has the right to be heard whenever he or she alleges mistreatment. A grievance process that affords employees the opportunity to air a complaint helps reduce dissatisfaction, identifies organizational problems, and improves morale.

The department retains the right under applicable laws and regulations to direct employees in the performance of their duties; to take the necessary means to achieve the proper ends under emergency situations; and to hire, promote, transfer, and assign employees as well as to suspend, demote, discharge, or take disciplinary action against employees when there is just cause.

## II. PURPOSE

The purpose of this policy is to establish grievance procedures for departmental employees to resolve disputes or complaints concerning the terms or conditions of employment.

## III. APPLICABILITY

All employees and reserve officers of the Teague Police Department.

## IV. WHAT IS GRIEVABLE

A grievance is a complaint or dispute of an employee relating to employment, including but not necessarily limited to the following:

- A. Disciplinary actions, including terminations (whether resulting from formal discipline, unsatisfactory job performance, or any other involuntary separation), demotions, and suspensions. (TEXAS BEST PRACTICES: 2.08)
- B. The improper application of personnel policies, procedures, rules and regulations, and ordinances and statutes.

- C. Acts of reprisal because of the use of the grievance procedure or of participation in the grievance of another employee.
- D. Complaints of discrimination based on race, color, creed, political affiliation, age, handicap, national origin, or sex.
- E. Intimidation because of participation or failure to participate in political activities.

## **V. WHAT IS NOT GRIEVABLE**

Management reserves the exclusive right to manage the affairs and operations of the department. Accordingly, the following complaints are not applicable under this order:

- A. Establishment and revision of wages or salaries, position classifications, or general benefits.
- B. Work activity accepted by the employee as a condition of employment, or work activity that may reasonably be expected to be a part of the job content.
- C. The measurement and assessment of work through a performance evaluation except where the employee can show that the evaluation was arbitrary or capricious.
- D. The contents of established personnel policies, orders, and statutes.
- E. Failure to be promoted except where the employee can show that established promotional policies or procedures were not followed or applied fairly.
- F. The methods, means, and personnel by which work activities are to be carried on.
- G. Dismissal, layoff, demotion, or suspension from duties because of lack of work, reduction in the work force, or job abolition.
- H. The non-disciplinary hiring, transfer, assignment, and retention of employees within the agency.
- I. The relief of employees from duties during emergencies.
- J. The city's financial, budgetary, accounting, compensation, and organizational policies and procedures.
- K. Oral reprimands, warnings, or written reprimands.
- L. Management of city employees, including the right to determine the duties to be included in a job classification
- M. The right of management to make personnel appointments in accordance with adopted selection policies and techniques.
- N. The right of management to determine the number of persons to be employed or retained as employees, including the right to lay off employees whenever it is deemed to be in the best


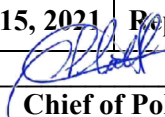
interest of efficiency or productivity or when necessitated by lack of funds or reduced workload.

- O. The right of management to establish rules and regulations governing work performance and conduct of performance evaluations
- P. The right of management to transfer and assign employees within the department; to determine the need for shift operation and rotation of the work week; to assign overtime; to determine job training and career development; and to determine duties or actions in emergencies.

## **VI. PROCEDURES**

Employees are encouraged to resolve grievances informally by discussing the matter with their immediate supervisor whenever possible. In the event such does not resolve the issue, this grievance procedure should be followed:

- A. Employees or recently separated former employees that are dissatisfied with any employment matter, including, but not limited to possible job discrimination, health and safety issues, or disciplinary actions, may pursue a grievance in accordance with this section.
- B. Employees or recently separated former employees must submit a written grievance regarding any employment matter to the City Administrator within seven (7) calendar days of the latest occurrence. A written grievance involving the City Administrator may be submitted to the Mayor or any council member but must be submitted within five (5) calendar days of the latest occurrence. The notice must specify what action was taken against the employee or what action has been observed, and how the action is either unwarranted or inappropriate.
- C. The City Administrator or a person appointed by the Mayor if the grievance is against the City Administrator, will investigate when necessary, allow the initiator of the grievance a reasonable opportunity to bring forth evidence and witnesses to support the initiator's case, and allow the initiator to question and fully refute any charges brought against the employee or recently separated former employee.
- D. The City Administrator or Mayor will determine if the matter should go before the Board of Aldermen, if any corrective action is necessary or if any disciplinary action should be pursued against perpetrators of any improper conduct complained of in the grievance. The Grievant will be notified in writing of the results of the grievance, and to the extent it does not violate privacy interests, the resulting action taken.
- E. Disciplinary action that has been taken against the employee by the Board of Aldermen is final and not subject to this grievance policy.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 4.7 Reserve Officer Program</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
	<b>Reference: TEXAS BEST PRACTICES 3.07 and 7.27</b>	

## I. POLICY

It is the policy of the Teague Police Department to maintain the highest standards of professional law enforcement services. Volunteers for reserve police officers must meet the same standards as other members of the organization. Reserve police officers should fulfill two primary functions. First, reserve officers serve as auxiliary manpower in situations as needed. Second, they provide an additional interactive link between the community and the police department. Reserve officers are subject to all the applicable rules and regulations that govern regular sworn personnel.

## II. PURPOSE

The purpose of this order is to describe the Police Reserve Unit, and outline its objectives, responsibilities, and operation.

## III. RESERVE PROGRAM (TEXAS BEST PRACTICES: 7.27)

### A. Requirements and certification

1. Requirements for age, education, and experience are the same as that for regular sworn personnel.
2. Applicants must meet all minimum requirements set forth by the Texas Commission on Law Enforcement Officer Standards and Education (TCLOE).
3. The selection process for reserve officer applicants is the same as for regular officers outlined in Policy 4.1 and 4.2.

### B. Certification and reserve officer levels

1. Apprentice Reserve Officers. Active reserve police officers who have obtained required peace officer training but have not completed field training.
2. Reserve Officer. Active reserve officers who have successfully completed basic peace officer certification, have completed field training, and hold basic peace officer license.

- a. Reserve officers will be assigned their duties on the reserve schedule. Reserve officers are required to provide 24 hours service per month.
- b. Reserve officers shall report to the supervisor or ranking officer for assignment duties and/or training.
- c. The on-duty patrol supervisor may, at his/her discretion, reassign the officer when personnel are required to assist in other areas.

### C. Training and Performance Standards

1. Reserve police officers serve at the discretion of the Chief of Police and may be called into service at any time the chief or his designee considers it necessary to have additional officers.
2. Reserve police officers shall be considered "on duty" when they are
  - a. performing "assigned duty"
  - b. representing or identifying himself/herself as a peace officer for the purpose of taking enforcement action or discharging legal duties.
3. All reserve police officers must serve a minimum of 24 hours of duty per calendar month. Officers who are unable to meet this requirement must submit a written request through the chain of command to the Chief of Police for an approved leave of absence.
4. Depending on the level of training and experience, reserve officers may perform the same duties as other full-time, sworn personnel or be assigned to work with a regular officer.
5. All reserve police officers are subject to the same rules, regulations, and orders as regular sworn personnel.
6. All reserve police officers must successfully complete the basic officer course required by TCOLE and obtain their license as a peace officer.
7. All active reserve police officers must successfully complete the police training officer program under the supervision and evaluation of a departmentally approved field training officer. Upon the successful completion of training, reserve officers will assume duties as designated by the Chief of Police.
8. For training and evaluation purposes, all active reserve officers will work one tour of duty with a field training officer within the first six months of each calendar year.


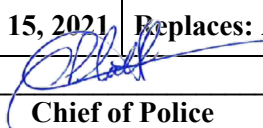
9. All reserve officers will be required to attend periodic in-service training to complete the following:
  - a. The same training as required of regular sworn officers including courses mandated by TCOLE for certification requirements; (TEXAS BEST PRACTICES: 3.07)
  - b. All departmentally required qualifications on firearms, the baton, and any other equipment deemed necessary.
10. Reserve officers are permitted to carry a weapon pursuant statutory law.

#### D. Chain-of-Command and Operations

1. The reserve unit functions as a unit of the patrol division and reports to sergeants of the patrol division. The sergeants may designate a patrol officer to serve as a reserve liaison to monitor reserve activities and assist the sergeant.
2. The sergeant supervising the reserve unit is appointed by the Chief of Police and shall be responsible for the overall administration and planning of the reserve unit.

#### E. Organizational Function

1. The primary function of reserve police officers will be to supplement patrol operations personnel.
2. Additionally, reserve officers will be on call for assistance in emergency situations such as disasters, riots, etc., and to provide additional manpower for special enforcement assignments.
3. All reserve police officer assignments will be coordinated through the office of the sergeant of the patrol division.
4. Reserve officers may, at the discretion of the Chief of Police, be assigned to other functions within the department depending on their skills and experience.
5. Reserve Officers are permitted to carry weapons off-duty, in compliance with statutory law and departmental policy.
6. Reserve Officers may enforce laws, on or off duty, in accordance with statutory law. Enforcement actions are governed by departmental policy and statutory law.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 4.8 Community Outreach and Customer Service</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
	<b>Reference: TEXAS BEST PRACTICES 2.24</b>	

## I. POLICY

It is the policy of the Teague Police Department to embrace the tenants of community policing and engage the community in a positive and trusting manner. Community involvement is essential to the successful operation of any police department. Without the assistance and acceptance of the community, a police agency’s effectiveness will not reach its full potential. Whenever possible, all avenues should be utilized in promoting the respect and cooperation of the public we serve.

All employees will extend reasonable assistance to the public. Reasonable assistance means the level of assistance that call load and current demand levels would permit. Employees must not neglect community services in the belief that the police function is restricted to crime control. It is the goal of the Teague Police Department to promote good relationships with the public and this goal can be facilitated by professional conduct and effective community outreach.

## II. PURPOSE

The purpose of this policy is to guide personnel and to affirm the department’s commitment to seek out opportunities to interact with the public and to build trusting relationships with the community. Feedback from the community and effective community outreach are expected from all employees.

## III. COMMUNITY OUTREACH

- A. Manager’s and Supervisor’s Role – Managers and Supervisors, by their words and actions, are to set the example for their subordinates in establishing and maintaining professionalism when interacting with the public and other employees.
1. All managers and supervisors shall ensure their employees maintain professionalism in their conduct and support them in promoting the respect and cooperation of the community in our daily contacts.
  2. Managers and supervisors are expected to keep their subordinates apprised of specific community problems and concerns.

3. Managers and supervisors should strive to cultivate avenues of communications with individual residents and groups within the community where they are assigned. Whenever practical, managers and supervisors should assign personnel to attend neighborhood meetings and civic functions.
4. Managers and supervisors are responsible to ensure that community feedback is sought by all personnel. (TEXAS BEST PRACTICES 2.24)
5. The Chief of Police (or designee) will coordinate the community surveys and approve the content of the questions.
6. Regardless of workload, the Chief of Police and all command staff are also expected to attend community meetings and to seek out opportunities to meet with all segments of the community.

#### B. The Employee's Role

No one can do more to foster positive police/community relations than the employee who is in contact with the public on a day-to-day basis. Employees must realize that their actions in every community contact have an impact on how the Teague Police Department is perceived by those we serve. Whenever possible, employees are expected to cultivate the respect and cooperation of the public through these contacts.

1. Employees shall provide reasonable assistance to all residents in need of service.
2. All personnel are expected to seek out opportunities to promote trust and positive dialog with the public.

#### C. Community Outreach

The Teague Police Department is committed to seeking out constructive community outreach programs that provide opportunities for members of the community and the police department to come together. Department employees are also expected to seek feedback from community members. If action plans or a new approach is needed to help solve a community concern, police personnel are expected to follow established internal protocols to recommend viable solutions.

1. Examples of Community Outreach Programs that are endorsed by this agency include, but are not limited to (TEXAS BEST PRACTICES 2.24):
  - a. Community forums
  - b. "Coffee with the Chief" meetings at local venues / restaurants
  - c. Open House at the main police headquarters


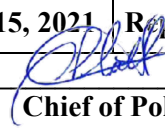


- d. Social media outlets
  - e. Officers eating lunch at area schools with students
  - f. Community surveys
  - g. Mentorship programs with local at-risk youth
  - h. Regular attendance at civic and religious functions
  - i. Infant seat installation safety checks
  - j. Citizens Police Academy
  - k. Back to school – shopping with a cop
  - l. Christmas with a cop – shopping with children
2. Community Feedback Mechanisms (TEXAS BEST PRACTICES 2.24)
- Seeking community feedback, and just as important - following up on the feedback, is crucial to the success of police community relations. The Teague Police Department is committed to actively seeking community feedback and whenever viable options for improvement can be found – to act on those findings. The following methods may be used to seek community feedback (with prior approval of appropriate city personnel):
- a. An annual survey may be placed in the water bill.
  - b. An electronic survey will be created and posted on the department website or Facebook page. The community will be encouraged by all personnel to take the survey and the Chief of Police (or designee) will seek out local media outlets to promote the survey.
  - c. All forums with the public will include a survey that can be submitted by those attending the meeting.
3. Social Media is an effective tool for community outreach; however, the Teague Police Department will not rely solely on this mechanism for community outreach (TEXAS BEST PRACTICES 2.24). It is important for all employees to seek out effective outreach programs that impact all segments of our community.
4. All survey results will be sent to the Chief of Police for review and action.

#### **IV. MANDATORY COMMUNITY OUTREACH ON IMMIGRATION STATUS**

It shall be the policy of this agency that community outreach shall be established regarding immigration status information.

- A. A peace officer may not inquire into the immigration status of a victim or witness to a crime unless the officer determines the inquiry is necessary to:
  - 1. investigate the offense; or
  - 2. provide the victim or witness with information about federal visas designed to protect individuals aiding law enforcement.
- B. Community outreach regarding immigration status shall include, but shall not be limited to, outreach to the following persons:
  - 1. Family violence, as that term is defined by Section 71.004, Family Code, including those receiving services at family violence centers under Chapter 51, Human Resources Code; and
  - 2. Sexual assault, including those receiving services under a sexual assault program, as those terms are defined by Section 420.003.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 5.0 Departmental Records</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: TEXAS BEST PRACTICES 5.01, 5.02 5.03 and 10.02 f</b>	

## I. POLICY

A “records unit” that functions well is critical for the effective delivery of law enforcement services. An efficient means of storing, cataloging, and retrieving records is essential for meeting the management, operational, and informational needs of the police agency.

## II. PURPOSE

The purpose of this policy is to assist records personnel in setting up and maintaining an effective record keeping system.

## III. RECORDS SECURITY (TEXAS BEST PRACTICES: 5.01)

- A. The police records are housed in a restricted area. Personnel assigned to the records unit are directly supervised by the Chief of Police.
- B. The records clerk is responsible for maintenance of department records and will be provided training in Law Enforcement Records Management and the Public Information Act.
- C. Access to the police records is restricted to assigned records personnel only. Entry by unauthorized personnel is prohibited.
- D. The departmental records will be secured and locked when it is not staffed by assigned records personnel.
- E. Personnel authorized by the Chief of Police may have access to departmental records after hours for need-to-know information only. Authorization may be granted to shift supervisors only.
- F. When entry has been made by authorized personnel, written notification to the records clerk will be made within 24 hours of the entry. Written notification must state the date entry was made, time entry was made, why entry was made, and what records were accessed and by whom.

#### **IV. RECORDING OF INCIDENTS BY CATEGORY**

A. To develop a comprehensive reporting system, it is necessary to record actions taken by law enforcement personnel whether in response to a request for service or for self-initiated actions. Each reported incident occurring within the department's service area will be categorized as one of the following and will receive a sequential incident or case number:

1. Individual's request for service, crime reports, or complaints that require one of the following:
  - a. an officer to be dispatched
  - b. an assigned employee to investigate
  - c. an assigned employee to act later.
2. Self-initiated criminal and non-criminal cases by officers.
3. Incidents involving arrests, citations (other than traffic), or summonses.

#### **B. Assignment of Case Numbers**

1. Officers will utilize the CopSync/Kologik software to assign case numbers to their call for service, which is required to be initiated when categorized by section "A" of this policy.
2. Case numbers are autogenerated through the CopSync/Kologik software system.
3. When a call for service is generated, the following information regarding that incident will be entered in the call for service fields:
  - a. Date and time of the initial reporting.
  - b. Name and address of the complainant or victim requesting the service.
  - c. Nature of the incident and the location.
  - d. Identification of the officers assigned to the call.
  - e. Time when officers were dispatched, arrived, and returned to service
  - f. Status, date, and time of action taken on the call.
  - g. Contact phone number, email, or address of complainant.

- h. A brief narrative to detail events of the call (what happened and what actions were taken).

#### C. Officer's Responsibilities

1. Officers will complete all required reports and turn them in to a supervisor prior to ending their shift.
2. Officers shall provide only a short summary narrative of the event on the call for service (who, what, when, and where). Details, including any listing of evidence, identification of witnesses, description of injuries, and any exculpatory information, shall be provided in an offense or incident report.
3. Supervisors will review all reports for accuracy and completeness and submit completed reports to the records unit before the end of shift.
4. Reports returned to officers for correction will be documented by the supervisor. Officers receiving a returned report shall make the necessary corrections and resubmit the report to their supervisor. At the next shift, the supervisor shall follow up, making sure that the report has been corrected and submitted.

#### D. Juvenile Records (TEXAS BEST PRACTICES: 10.02 f)

1. A file is maintained on each juvenile (ages 10 to under 17) arrested, referred, or detained by an officer. The file includes all documents associated with the contact as indicated in this section, as well as a running list of the juvenile's detentions and dispositions.
2. State and federal laws require that juvenile files be kept separate from adult files.
3. Juvenile fingerprints and photographs, if any, will be turned over to the Juvenile Probation Department intake officer.
4. Police records will not maintain fingerprints or photographs of juveniles. Should fingerprints or photographs be turned over to police records they will be destroyed as specified in the Family Code sections 58.001 and 58.002.

#### E. Computerized Criminal History Information

1. Computerized criminal history information (CCH) is a federal/state cooperative system of a variety of databases (arrests, convictions, driving records, outstanding warrants, and others). The CCH database lists all arrests and convictions for offenses above Class C misdemeanor that have not been purged in accordance with state/federal age purge criteria.

2. Access to the TCIC/NCIC criminal history database is limited to designated personnel. The program generates its own log showing who accessed the system. The log is computerized and maintained by information systems personnel.
3. Access to CCH information through local law enforcement agencies is limited to criminal justice uses.
4. Individuals who request a copy of their computerized criminal history must do so through the Texas Department of Public Safety in Austin.
5. Numerous agencies have been given authority to access criminal history information on prospective licensees or applicants. The statutes giving this authorization do not permit use of local police agency TCIC/NCIC lines for obtaining the CCH. Requests of this nature are to be referred to a clerk.

## **V. REPORT NUMBER AUDIT AND REPORT STATUS**

- A. The records clerk will run an audit daily to ensure that all reports have been turned in to the records department. As documents are received the reports will be placed in numerical order by service number.
- B. When a report has not been turned in within three days of the incident, a printout of the audit report is made, and one copy kept for follow up. The officer responsible for the report will be identified and the audit report will be sent to the officer for response. Follow-ups for missing reports will be made daily until all missing reports are accounted for.
- C. When a report has not been received within 72 hours after the end of the shift on which the call was taken, a missing-report notice will be sent to the officer, the officer's clerk, and the Chief of Police.

## **VI. DISTRIBUTION OF REPORTS AND RECORDS**

- A. After reviewing the reports for completeness, the patrol supervisor will forward all reports and citations to the records unit.
- B. Originals are maintained in the records unit filing system.
- C. Citations are electronically entered into the CopSync/Kologik software system and forwarded to the municipal court. A printed and signed copy of the citation will be submitted to the shift supervisor and forwarded to the Municipal Court, after review for correctness.

## **VII. RECORDS RETENTION AND DESTRUCTION (TEXAS BEST PRACTICES: 5.02)**

- A. Records will be retained in the records unit as specified in this policy until they are purged or destroyed in accordance with the approved City Records Retention Policy or statutory law applicable and any court orders requiring them to be expunged.
- B. Accident Reports: Files are maintained electronically through the Texas Department of Transportation online CRASH reporting system. A courtesy copy is printed and maintained by the records department. These courtesy copies will be maintained for a period of 2 years. Persons wanting accident reports after the 2-year retention may order a copy directly from the Texas Department of Public Safety or the Texas Department of Transportation.
- C. Offense Reports: Because some offenses do not have a limitations period -- they can be prosecuted at any time -- because the limitations period for some offenses is based on the age of the victim at the time of the offense, offense report purging cannot be based solely on a calculation of the number of years from the date of the offense. Careful consideration will be given to these circumstances during the records retention process.
- D. All Other Information Reports: The originals of miscellaneous incident reports will be kept for an indefinite period, and they will be kept in numerical order just as offense reports are kept.
- E. Adult Arrest Files: Adults may obtain a court order to have their arrest records expunged as specified in Chapter 55 of the Code of Criminal Procedure. If no such order is obtained, adult arrest files will be kept until there is a report of the death of the arrestee or for a period of 75 years.
- F. Juvenile Arrest Files: (TEXAS BEST PRACTICES: 10.02 f)
  - 1. A juvenile arrest file will be created for every juvenile taken into custody by members of this department. Juvenile files are maintained separately from adult files and, like all files, are kept secure from unauthorized disclosure.
  - 2. Persons may have their juvenile records sealed (not destroyed) by court order as specified in Family Code section 58.003.
  - 3. A court may order destruction of juvenile detention files as specified in Family Code section 58.006.
  - 4. Arrest report files on juveniles who were referred to juvenile court may be purged after the person reaches the age of 23.
  - 5. Arrest report files on juveniles who were not referred to the juvenile court may be purged after the person reaches the age of 18.
  - 6. As specified in Chapter 58 of the Family Code, police records will not maintain fingerprints or photographs of juveniles because the juvenile was detained by police or suspected of a criminal offense. Fingerprints and photographs taken as part of the

juvenile intake process will be turned over to juvenile probation department officials. Should it happen that fingerprints or photographs have been turned over to the records unit they will be destroyed as specified in Family Code sections 58.001 and 58.002.


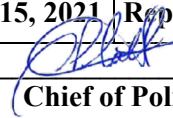
7. Any juvenile records that are in a gang or criminal street gang intelligence file will be maintained, managed, and removed pursuant to the Texas Code of Criminal Procedure Articles 61.04 and 61.07.
- G. Destruction of files and records will be done by shredding, burning, or other means of destruction approved by the City of Teague City Secretary, when documents have been held beyond the required retention schedule.

### **VIII. UNIFORM CRIME REPORT (UCR)/National Incident Based Reporting System (NIBRS) AND RELEASE OF RECORDS (TEXAS BEST PRACTICES: 5.03)**

- A. It is the responsibility of the Chief of Police (or designee) to complete the monthly UCR/NIBRS and monthly council report in a timely manner.
- B. The Chief of Police (or designee) must read and be familiar with the UCR/NIBRS handbook, including all UCR/NIBRS reporting standards. Training is available through the Texas Department of Public Safety and must be completed before being authorized to compile these reports.
- C. The Chief of Police (or designee) must perform several audit checks for each crime reported.
- D. The Texas Public Information Act governs release of information reported to law enforcement agencies.
- E. Any request for information contained in any report made or compiled by the department is to be referred to the City Secretary. The Chief of Police or records clerk will prepare a copy of the requested information and forward to the City Secretary for review, before being released.
- F. Under no circumstances should a release of records be made without the approval of the City Secretary if such records are being requested pursuant Public Information Act.
- G. All arrest files maintained in the records files and the computer will be the responsibility of the records clerk. Copies of files will be released only to the following authorized persons:
  1. Personnel of this department.
  2. Sworn officers from other agencies upon written request.
  3. Courts of law under proper process.



4. District attorneys.
  5. Federal law enforcement agencies.
  6. Probation departments.
  7. Military personnel with a written request and signed waiver of the named person. Copies of waivers will be kept for a period of three (3) years.
- H. Juvenile arrest information is closed to public information requests and will not be released without a court order or signed waiver from the juvenile and a parent or guardian.
- I. Original reports will be released only to members of this department but should not leave the premises unless doing so is following a court order or authorized by the Chief of Police. Every release will be documented in the records check-out log, showing the date, name, file name and number, and the name of the clerk releasing the files. A copy of the report will be made prior to release of any original report. Upon the return of original records, the records clerk will review the contents of the return against the “check-out log,” checking for discrepancies. The records clerk will note who returned the files, as well as the date and time. If there are no discrepancies in the contents of the records being checked in, the receiving person will initial the “check-out log” and return the record to its original file location.
- J. Records personnel, after reviewing with the Chief of Police, will respond to all requests from the courts for original records. A complete copy of the requested records will be made before they are removed from the original records unit.
- K. Any individual may request a “clearance letter” for several purposes, such as travel visas and adoptions. Such a letter must be submitted to records personnel along with at least two pieces of identification, one of which must include a photo. Records personnel will check local records only. Records personnel will prepare a “To Whom It May Concern” letter indicating that no criminal record has been recorded in the City of Teague. The individual makes state or federal criminal history inquiries directly to those agencies.

	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 5.1 Media and Public Information</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____ <div style="text-align: center; margin-left: 150px;">   <b>Chief of Police</b> </div>
	<b>Reference:</b> TEXAS BEST PRACTICES 5.03 and 5.04

## I. POLICY

This agency must have the support of the community to be successful. Establishing and maintaining an effective relationship with the news media is crucial to accomplishing this goal. A positive working relationship with the media is mutually beneficial. It shall be the policy of this agency to cooperate with the news media and to maintain an atmosphere of open communication. To this end, information shall be released to the news media in an impartial, accurate, and timely fashion. It shall be the responsibility of each employee to abide by this philosophy of cooperation.

## II. PURPOSE

The purpose of this policy is to establish guidelines regarding media relations and the release of information to the public through the news media.

## III. RESPONSIBILITIES IN RELEASING INFORMATION

- A. The Chief of Police may designate any member of the department as the Public Information Officer (PIO) for the department. The PIO is the primary contact for the news media. In the event a PIO has not been designated or if he/she is unavailable, the Chief of Police is responsible for PIO duties.
- B. Supervisors with responsibility for a specific case or incident may be the secondary contact for the news media with the approval of the Chief of Police.
- C. The Chief of Police may direct other employees to respond to media inquiries.

## IV. TRAINING

This agency is committed to providing proper training for its public information officer. Supervisors, line officers, and other personnel who interact with the media shall also be provided appropriate training in media relations and the Public Information Act.

## V. PROCEDURES

A. Media Requests: The agencies will respond to all media inquiries in a timely and professional manner.

1. During normal business hours, media inquiries shall be directed to the Chief of Police.
2. No employee shall release any information that would jeopardize an active investigation, prejudice an accused person's right to a fair trial, or violate the law.
3. The Chief of Police or PIO shall be responsible for assisting the news media by conducting interviews or coordinating interviews with other qualified agency personnel.
4. Employees contacted directly by the media requesting an interview shall refer them to the Chief of Police and immediately notify the Chief of Police of this request.
5. All conversations with members of the news media should be considered "on the record" and subject to being quoted.

B. News Releases

1. News releases shall be written and disseminated to the media and to agency employees on major incidents and events of community interest or concern.
2. The Chief of Police or appropriate designee will write the news release.
3. The Chief of Police, or designee, will approve all news releases.
4. News conferences shall be held only in connection with major events of concern to the community.

C. Access to Crime Scenes and Critical Incidents

1. Agency personnel shall be courteous to news media representatives at crime and critical-incident scenes.
2. At such scenes, agency personnel shall ensure that the media respect the established perimeter.
3. In general, members of the media shall receive no more and no less access to an incident scene than members of the public. However, the Chief of Police or PIO designee may allow news personnel and their equipment closer access to a crime or critical-incident scene so long as the degree of closeness does not interfere with law enforcement operations.

4. No member of this agency shall prohibit the media from news-gathering practices, including photography and interviews, outside the established perimeter of a crime scene or critical-incident scene.
5. News media representatives shall not be prevented from access to any area solely because of the possibility of their injury or death. If this is the only consideration, the scene commander shall advise the media representative of the danger and allow the media representative to make the decision to enter on his or her volition.
6. Only the Chief of Police or PIO designee shall release information to the news media at crime and critical incident scenes.
7. At critical incident scenes, the Chief of Police or PIO designee shall establish a media briefing area as close to the scene as safety and operational requirements allow.
8. At critical incident scenes, members of the agency shall work in close cooperation with the media to ensure that live broadcasts do not disclose any information that could endanger law enforcement personnel or the public.

#### D. Access to Suspects

No member of this agency shall pose any suspect or accused person in custody or make him or her available for media interviews.

#### E. Joint Investigations or Operations Involving Another Agency

In a multijurisdictional investigation, the lead investigative agency is responsible for providing or coordinating the release of public information. The PIO or designee for the lead agency should share that information with all involved agencies in advance of public dissemination.

## **VI. INFORMATION RELEASE GUIDELINES**

- A. The release of information is subject to restrictions placed by applicable state and federal laws.
- B. No member of this agency shall release any information that would hamper the successful conclusion of an investigation or jeopardize the safety of affected persons.
- C. Agency members can release the following information:
  1. Basic information about a crime or incident.
  2. Basic information about victims, except as excluded by law.

3. Description of suspects.
4. Basic description of weapons and vehicles used.
5. Basic description of stolen items.
6. Basic description of injuries and condition of victims.
7. The basic information about arrestees and the charges against them.
8. Information contained in arrest affidavits and other applicable crime or incident reports.
9. Booking photographs.

D. Agency members shall not release the following information:

1. Names, addresses, or any other information that would identify the victim of a sex offense, child abuse, or any other crime where the privacy of the victim is protected by law.
2. Names, addresses, and basic information about juvenile arrestees, as governed by state law.
3. Active criminal investigative information, active criminal intelligence information, and surveillance techniques.
4. Names of informants and information provided by them.
5. Supplemental or investigative reports until such time as the case is closed or the Chief of Police deems it permissible.
6. Grand jury testimony and proceedings.
7. Active internal affairs investigations, as governed by state law.
8. Names of witnesses, unless required by state law.
9. The identity of critically injured or deceased persons prior to notification of next-of-kin.
10. Home address, telephone numbers, and familial information of law enforcement personnel.
11. Names of undercover personnel.


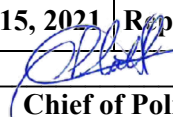
12. Any other information that could jeopardize the successful conclusion of an investigative and prosecution.

13. Any other information prohibited by state law from public disclosure.

## **VII. SOCIAL MEDIA SITES**

A. The Chief of Police of designated Public Information Officer shall be responsible for operating, managing, and monitoring all department-sponsored social media sites.

B. Operation of the social media sites shall be in accordance with Policy 2.8 Use of Social Media.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 5.2 Computer and Electronic Equipment Usage and Data Security</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 _____ <b>Chief of Police</b>
	<b>Reference:</b>	

**I. POLICY:**

It is the policy of this department to ensure proper use of electronic computing and recording systems by establishing authorized uses and users. It states the protocols for storage, security, and retention. It also establishes what uses of such equipment are prohibited and what constitutes inappropriate use of such equipment. Body Worn Cameras are provided to officers as a supplemental device that will extend the video recording and audio recording capability to be used in the field.

**II. PURPOSE:**

It is the purpose of this policy to define and provide clear direction as to the allowed uses and the prohibited uses of departmental and personal electronic computing and recording equipment, to provide for data security and retention periods, and to establish protocols for proper handling of digital evidence.

**III. DEFINITIONS**

- A. Network Terminals: Desktops, laptops, or any other electronic devices that connect to the department’s internal computer network.
- B. Mobile Digital Computers (MDC): In-vehicle computers or any other electronic devices that in some manner connect to the Internet, department computer networks, or other service, such as TCIC, that provides officers with data or allows officers to conduct field reporting or communications with other officers or the department.
- C. Mobile Phones: Either department owned or personally owned cell phones or smart phones.
- D. Body Cameras / Digital Media Recorders (DMR): Video/Audio recordings made via a camera system that is worn by police personnel.
- E. Mobile Video Recording: In-vehicle camera systems that are permanently mounted in department vehicles.
- F. Digital Media Recorder (DMR): Officer-worn digital audio or video recording device.

- G. Digital Camera: A single-purpose, handheld camera designed to take digital photographs.
- H. License Plate Reader: Vehicle-mounted or handheld digital camera system that identifies and captures license plate numbers and locations.

#### **IV. PROCEDURES:**

The sections below outline the procedures to be used and list the specific prohibitions regarding the use of specific equipment.

##### **A. General Provisions**

1. Any electronic document, report, audio, or video recording, image, email, voice communication, or any other form of electronic data created while on or off duty that is directly related to official department operations or investigations, whether created on personal or department-owned equipment, is considered to be a government record. As such, it is subject to public record laws, and it shall be preserved accordingly.
2. Anything that is created on department-owned equipment, whether or not it is directly related to official department operations or investigations, may be considered a government record, and may be reviewed and shall be preserved as required by state law or department policy. This includes any electronic document, report, audio or video recording, image, email, voice communication, and any other form of electronic data created while on or off duty.
3. All department-owned equipment and its use are subject to routine or specific review and/or investigation by department supervisors as needed to ensure appropriate use.
4. On-duty use of any electronic device, such as a mobile phone or phone camera, for strictly personal purposes not related to departmental operations is generally considered private unless the information would tend to show inappropriate activity. Off-duty use of personal electronic devices is also generally considered private unless the use results in a violation of departmental general orders or state or federal law.
5. All employees that directly access the TCIC/NCIC database will be trained in the appropriate level of access.
6. If any form of digital evidence exists, formal departmental reports will include a notation that such evidence exists, including the type of evidence and the storage location.



## B. General Prohibitions

1. Employees will not release, share, or make copies of any electronic documents, reports, audio or video recordings, images, emails, voice communications, or any other form of electronic data created while on or off duty that is directly related to official department operations or investigations, whether created on personal or department-owned equipment, unless specifically authorized by this order or the Chief of Police.
2. Employees will not use department-owned equipment, electronic or otherwise, for personal benefit or to conduct personal business.
3. Employees can access the internet for personal use during meal and other breaks if the sites accessed are appropriate for public viewing. An officer can be questioned about his/her internet activities by defense counsels in criminal trials, potentially damaging the officer's credibility as a witness.
4. No video games will be played on department equipment.
5. No inappropriate websites will be visited.
6. Inappropriate use of electronic devices or the release or posting on the internet or various social media sites of another party's private information, or governmental information usually deemed private can lead to internal investigations and subsequent disciplinary action.

## V. DEPARTMENT NETWORK TERMINALS

### A. Security

1. The department has several computers, and other devices, throughout the department that have access to the department network. All employees will be issued a unique login ID and password to allow access to the system.
2. Employees will safeguard their login ID and password to ensure no other person will gain access using their login ID and password.
3. Employees will not leave a computer connected to the network with their login ID and password, if they are not physically able to prevent access by visible monitoring of the computer.
4. Employees are responsible for all access to the network using their login information.
5. The department will assign appropriate security levels, within the network, to allow access to certain files only as required.

## B. Required Access

1. All employees are required to sign into the network at least twice each workday (at the beginning and end of their shifts).
2. Employees must read and respond to all department emails and training assignments, each day they are assigned a duty status.
3. Employees who discover network terminals in need of repair will notify their Supervisor as soon as possible.

## **VI. MOBILE DIGITAL TERMINALS / COMPUTERS – MDT/MD**

- A. The Mobile Data Terminal/Computer (MDT/MDC) is a part of the radio system, which uses frequencies licensed by the FCC. Rules concerning proper radio procedures also apply to use of the MDT.
- B. Messages (1) will not be personal, (2) will not contain derogatory references to other persons or agencies, and (3) will not contain any text that a reasonable person would find offensive. These messages are subjected to Open Records laws.
- C. Using the MDT/MDC, field officers may signal (1) receipt of a call for service, (2) arrival at the scene of a call, (3) request for assistance, and (4) clear from a call, but they shall also do so by voice communications so that other field units and supervisors will be kept aware of ongoing operations.
- D. Because messages sent with the CAD/MDT system slow the system's response time, only concise, work-related messages may be transmitted. Personnel are urged to use abbreviations to help keep the messages brief.
- E. There is NO EXPECTATION of privacy concerning sending or receiving messages via the CAD/MDT system.
- F. Except in emergency situations or in single-key response to dispatched calls or enquiries, the driver of the vehicle will not utilize the MDT/MDC keyboard while the vehicle is in motion. Drivers will pull to a safe location before utilizing the keyboard.

## **VII. MOBILE VIDEO RECORDING SYSTEMS**

- A. The use of a Mobile Video Recording (MVR) system provides persuasive documentary evidence and helps defend against civil litigation and allegations of officer misconduct. Such evidence is often used in court cases and can help in determining the guilt or innocence of accused people.
- B. Officers assigned the use of these devices shall adhere to the operational objectives and protocols outlined herein to maximize the effectiveness and utility of the MVR and the integrity of evidence and related video documentation.

### C. General Procedures

1. It shall be the responsibility of this department to ensure that the audio-video recording equipment is properly installed according to the manufacturer's recommendations.
2. MVR equipment shall automatically activate when emergency equipment (lights) or a wireless transmitter is operating.
3. The system may also be activated manually from the onboard computer system, which has the control panel for the video system.
4. Placement and operation of system components within the vehicle shall be based on officer safety requirements.
5. All officers shall successfully complete this department's approved course of instruction (Field Training) prior to being deployed with MVR systems in operational settings.
6. Inspection and general maintenance of MVR equipment installed in departmental vehicles shall be the responsibility of the officer assigned to the vehicle.
7. Prior to beginning each shift, the assigned officer shall perform an inspection to ensure that the MVR is performing in accordance with the manufacturer's recommendations covering the following matters:
  - a. Remote activation of system via transmitter
  - b. Windshield and camera lens free of debris
  - c. Camera facing intended direction
- d. Recording mechanism capturing both audio and video information, that is, the system plays back both audio and video tracks.
  1. Malfunctions, damage, or theft of in-car camera equipment shall be reported to the immediate supervisor prior to placing the unit into service.
  2. Mandatory Use:
    - a. All official contacts whether on a call or officer initiated
    - b. Traffic stops (to include, but not limited to, traffic violations stranded motorist assistance, and all crime-interdiction stops)
    - c. Priority responses

- d. Vehicle pursuits
  - e. Prisoner transports
3. When the MVR is activated, officers shall ensure that the audio portion is also activated, via the body mic, so that all events are properly documented. Officers are encouraged to narrate events using the audio recording, which will provide the best documentation for pretrial and courtroom.
  4. Officers using the body mic transmitters, which are individually synchronized to their MVR, shall activate both audio and video recordings when responding in a support capacity to obtain additional perspectives of the incident scene.
  5. When officers park patrol units in their designated parking place, the MVR downloads automatically to the server and is maintained by the Chief of Police.
  6. Officers shall not erase, alter, reuse, modify, or tamper with MVR recordings.
  7. When the MVR is activated to document an event, it shall not be deactivated until one of the following has occurred:
    - a. the event has been concluded,
    - b. the intention to stop the recording has been noted by the officer either verbally or in a written notation.
  8. Supervisor Responsibilities
    - a. All recordings are maintained on the departmental server.
    - b. The supervisor shall periodically check the server to ensure recordings are being downloaded.
    - c. Supervisors who are informed or otherwise become aware of malfunctioning equipment shall ensure that authorized personnel make repairs in a timely manner.
    - d. Supervisors shall conduct periodic reviews of officer-assigned media to periodically assess officer performance.
    - e. Supervisors will assure proper functioning of MVR equipment and determine if MVR equipment is being operated properly.
    - f. Supervisors will identify recordings that may be appropriate for training.
    - g. Supervisors shall conduct bi-weekly reviews of personnel who are newly assigned MVR equipment to ensure compliance with departmental policy.

- h. Supervisors shall conduct quarterly reviews.
- i. Minor infractions (not criminal in nature) discovered during the routine review of recorded material should be viewed as training opportunities and not as routine disciplinary actions.
- j. Should the behavior or action persist after it has been informally addressed, the appropriate disciplinary or corrective action shall be taken.

## **VIII. MOBILE TELEPHONES**

### **A. Department Issued Cell Phones**

- 1. Cell phones are issued by the department to increase the level of communication between field officers and the department as well as citizens.
- 2. Cell phones are to be used for appropriate departmental activities only.
- 3. Employees can use department cell phones for emergency and short personal calls during breaks.
- 4. The department regularly inspects cell phone usage records for inappropriate activity.

- B. Cell Phones Personally Owned: The department allows employees to carry personally owned cell phones for emergency contact purposes. Use of personal phones, while on duty, should be limited, to not interfere with assigned duties. At no time should a personally owned cell phone be used for any part of official duties (Scene Photos, Video/Audio recordings, etc.) and are to remain inside their patrol vehicle while handling calls for service. Using personally owned cell phones for official duties may subject the phone to open records request and being subpoenaed to court (civil or criminal).

## **IX. CELL PHONE CAMERAS**

### **A. Departmental Cell Phones**

- 1. Cell phone cameras, both still and video, may be used to record department activities only when another more suitable camera or recording device is unavailable.
- 2. Activities may include victim, witness, or suspect information, crime scenes, field and eyewitness identifications, witness statements, etc.
- 3. All activities recorded on cell phone cameras will be transferred immediately to departmental records systems as soon as the incident can be concluded and no later than the end of shift. Appropriate information technology staff will be consulted regarding the safest transfer method.

## B. Personal Cell Phones

Personal cell phones should not be utilized for any official business of this department.

## X. DIGITAL CAMERAS

### A. Department Issued Cameras

1. Personnel are assigned appropriate camera systems for recording crime scenes and incidents.
2. Department-issued cameras will not be used for any personal use.
3. All images or data recorded will be transferred to appropriate departmental media or storage before the end of shift.

### B. Cameras Personally Owned

1. No employee will carry or use a personally owned camera on duty

## XI. DIGITAL MEDIA RECORDERS (Body Worn Audio/Video Recorders)

Note: These procedures do not apply to mounted in-vehicle audio/video systems, which are covered elsewhere in this order.

### A. POLICY

It is the policy of the Teague Police Department that all sworn members comply with the following procedures for the use and maintenance of the Body Worn Cameras (BWCs). This policy will cover any recordings of audio and video captured by use of the BWC

### B. DEFINITIONS

1. BODY WORN CAMERAS or (BWC) -- are camera systems designed to be worn by police officers to capture digital multimedia evidence.
2. DIGITAL MULTIMEDIA EVIDENCE or (DME) -- consist of all digital recordings to include by not limited to audio, video, photographs, and their associated metadata.
3. METADATA -- includes any digital identifiers that are captured as part of the actual recording, such as date & time, GPS coordinates, labeling, etc.

### C. PROCEDURES

1. Prior to using a BWC, officers shall receive Department-approved training on its proper operation, care, and the department's policy with respect to the use of the BWC. Additional training shall be provided at periodic intervals to ensure the

continued effective use of the equipment, proper calibration/performance; and to incorporate changes, updates or other revisions in policies or equipment.

2. BWC's and equipment should be used with reasonable care to ensure proper functioning. Equipment malfunctions shall be brought to the attention of the officer's supervisor as soon as possible so that a replacement unit may be assigned. Officers shall inspect and test BWC's prior to each shift to verify proper functioning and shall notify their supervisor of any problems. Department Issued Digital Media Recorders (DMR).
3. In the event a BWC is lost, upon discovery the officer shall immediately notify their supervisor.
4. Officers shall wear BWC's above the midline of their torso and in position designed to produce an effective recording.
5. Officers shall not use BWC's personally owned while on duty.
6. Officers assigned a BWC may use the camera at approved off-duty employment, but only in conjunction with their official duties. If used for this purpose, the officer shall download all Digital Media Evidence during their next regularly assigned on-duty shift.

#### D. BACKGROUND

1. Body Worn Cameras are an affective law enforcement tool that can reduce violent confrontations and complaints against officers. Body Worn Cameras provide additional documentation of police-public encounters and may be an important tool for collecting evidence and maintaining public trust.
2. This policy is intended to provide officers with instructions on when and how to use Body Worn Cameras.
3. The Department has adopted the use of body worn cameras to accomplish several objectives; including, but not limited to:
  - a. Body worn cameras allow for accurate documentation of police-public contacts, arrests, and critical incidents. They also serve to enhance the accuracy of officer reports and testimony.
  - b. Body worn cameras allow for accurate documentation of police-public contacts, arrests, and critical incidents. They also serve to enhance the accuracy of officer reports and testimony.
  - c. Audio and video recordings enhance the Department's ability to review probable cause of arrest, officer and suspect interaction and evidence for investigative and

prosecutorial purposes and to provide additional information for officer evaluation and training.

- d. Body worn cameras may also be useful in documenting crime and accident scenes or other events that include the confiscation and documentation of evidence or contraband.
- e. The Department recognizes that video images cannot always show the full story nor do video images capture an entire scene. The use of body worn cameras does not reduce the requirement to provide thorough written documentation of an incident. Persons reviewing recordings must also be cautious before conclusions are reached about what the recordings show.

#### E. OVERVIEW

1. The body worn cameras should be utilized to:
2. Collect evidence that can be used in the prosecution of criminal offenses.
3. Record contacts with the public to secure unbiased evidence in connection with investigations.
4. Allow for supervisory review to ensure that the department policies and procedures are followed as they relate to the use of BWC's, and
5. Capture footage that would be helpful for training.

#### F. LEGAL ISSUES.

1. BWC equipment and all data, images, video, and metadata captured, recorded, or otherwise produced by the equipment is the property of the Department. The personal use of all information recording by BWC's shall be pursuant to the prior written approval of the Chief or his designee.
2. Use of BWC's for any purpose other than in accordance with this policy is prohibited.
3. All data, images, video, and metadata captured by BWC's are subject to state statutes regarding retention of records.

#### G. OPERATION OF BODY WORN CAMERAS (BWC's)

1. Except as otherwise provided in this policy and with limited exceptions, officers shall be required to activate their BWC's when responding to all calls for service and during all law enforcement-related encounters and activities that occur while the officer is on duty. Examples include but are not limited to:



- a. All calls for service in which official contact is made with citizens
  - b. All traffic stops
  - c. All citizen transport (excluding ride-a-longs)
  - d. All investigatory stops
  - e. All foot pursuits
  - f. Arrests of any person(s)
  - g. Searches of any kind
  - h. Seizures of any evidence
  - i. Request for consent to search
  - j. Miranda warnings and response from in custody suspects
  - k. Statements made by citizens and suspects
  - l. K-9 searches of vehicles, businesses, homes, or other areas
  - m. Issuances of written violations
  - n. Arriving at law enforcement events and/or citizen contact initiated by other officers
  - o. Other incidents the officer reasonably believes should be recorded for law enforcement purposes.
2. Officers have no obligation to stop recording in response to a citizen's request if the recording is pursuant to investigation, arrest, lawful search, or the circumstances clearly dictate that continued recording is necessary. However, officers should evaluate the situation and when appropriate, honor the citizens' request. The request to turn off the BWC should be recorded as well as the officers' response.
3. Officers who stop recording an incident for any reason shall:
    - a. Articulate verbally on camera their reasons, i.e., unsafe impossible or impractical.
    - b. Officers shall also articulate in their written report their reasons for stopping or not recording public contacts.

## H. Officer Responsibilities

1. Officers issued a department owned DMR shall attend training, and they will demonstrate proficiency with the recording and transfer of recorded data.
2. Officers shall inspect the device at the beginning of each shift to ensure proper operation, including sufficient battery life and recording medium.
3. Any device found deficient at any time will be immediately reported to the officer's supervisor who will issue a replacement if one is available.
4. Any DMR data created will be downloaded or copied to the appropriate department storage location before the end of shift.
5. Much of the recorded data will not be needed – as in a building search where nothing is found, or a citizen contact that did not result in any action. But any data that an officer believes might be evidence or is likely to be needed for any other purpose, such as a potential employee complaint, should be noted in official reports. If the recording may be needed and no report is made, the officer should contact the DMR manager, so the data may be flagged and kept secure as needed; however, all recorded data will be held in accordance with applicable laws

## I. Digital Media Recorders Personally Owned– DMRs

Department personnel are prohibited from using personally owned DMRs in the course of their official duties.

## J. Deactivation of the BWC shall occur when:

1. The event has concluded.
2. Victim and/or witness contact has concluded.
3. All persons stopped have been released.
4. Once an arrestee has been placed into a vehicle to be transported to the Detention Center. However, the officer transporting the arrestee to the detention center shall keep their BWC activated until custody of the individual is transferred to the Detention Center.
5. If an officer fails to activate a body worn camera, or fails to record the entire contact, the officer shall document the reasons for doing so on the Form ONE or Incident report.

6. Officers shall not activate BWC's when engaged in conversations with individuals with whom the officer is in a privileged relationship i.e., spouse, attorney, peers, chaplain, etc.
7. Officers shall not edit, alter, erase, duplicate, copy, share or otherwise distribute in any manner BWC images and information without prior written approval of the chief or his designee.
8. Officers shall be allowed to review the recordings from their BWC's at any time. To help ensure accuracy and consistency, officers are encouraged to review recordings prior to preparing reports. If the officer is giving a formal statement about the use of force or if the officer is subject to a disciplinary investigation, the officer shall:
  - a. Have the option of reviewing the recordings in the presence of their attorney; and
  - b. Have the right to review recordings from other BWC's capturing the officer's image or voice during the underlying incident.

K. BWC's shall not be used to record:

1. Communications with other police personnel. Officers shall not intentionally create digital recordings of other employees in areas where a reasonable expectation of privacy exists.
2. Officers shall not knowingly record encounters with undercover officers or informants.
3. When an officer is on break or is otherwise engaged in personal activities.
4. Officers shall not intentionally create digital recordings of citizens' activities in areas where a reasonable expectation of privacy exists, unless the recording is made while the officer is legally in the area for one of the situations listed in section B above.
5. When an officer would be recording a patient during a medical or psychological evaluation by a clinician or similar professional, or during treatment. When recording in hospitals or other medical facilities, officers shall be careful to avoid recording persons other than the suspect. This does not prohibit the recording of medical events as a direct response for calls for service, i.e., overdoses, accidents, etc.
6. Communications made in a psychiatric facility, unless responding to a call involving a suspect who is thought to be present in the facility.
7. Officers may use BWCs in patient care areas of hospitals or emergency rooms when the recording is for official business.

8. To the extent possible, officers will attempt to prevent the recording of non-involved individuals.

#### L. Supervisor's Responsibilities

1. Supervisors will attend department training on the use, retrieval, and storage of data, using BWCs.
2. Supervisors will take such action to ensure data from BWCs is transferred and stored properly and in a timely manner.
3. Supervisors will remind officers of rules regarding BWC evidence on a regular basis.

#### M. HANDLING OF DIGITAL MULTIMEDIA EVIDENCE (DME)

1. All files from BWC's shall be securely downloaded no later than the end of the officers' shift. Each file shall contain information related to the date, BWC identifier, call for service numbers and assigned officer. Files shall be treated as "evidence" until otherwise determined by records retention or court ordered destruction.
2. All files from BWC's shall be securely stored in accordance with state records retention laws and for no longer than useful for purposes of training, or for use in investigation or prosecution (including appeals), or for use in resolving a claim, pending litigation or disciplinary investigation. In capital punishment prosecutions, files shall be kept according to state retention policy.
3. It is not the intent of the Department to review BWC for the sole purpose of general performance evaluations. Supervisors and internal affairs personnel may access BWC for administrative investigations. Other than periodic supervisory reviews to ensure that equipment is functioning properly, the scope of the review of BWC should be limited to the specific complaint against the officer. Inadvertent discovery of other allegations during this review shall require the supervisor to articulate the purpose of expanding the scope.
4. Requests for deletion of portions of a recording from a BWC (i.e., in the event of a privileged or personal recording) must be submitted in writing to the chief or his designee.
5. Officers shall not allow any person outside this department to view the BWC or any other recorded data without the permission of the Chief of Police.
6. Uploading of any BWC data to any social media site is prohibited.
7. Recordings from BWC's may be shown for training purposes upon completion of a criminal case. All such use shall be pursuant to the written authority of the chief. Officers shall be provided with written notice if recordings intended for use for

training purposes were either made by them or captured their image or voice as a courtesy. All recordings are the sole property of the Department.

#### N. RETENTION & DESTRUCTION OF DIGITAL MULTIMEDIA EVIDENCE (DME)

1. The retention and destruction of DME shall follow the guidelines set forth by Texas State laws and City of Teague and Police Department Policies.
  - a. Class C misdemeanors and unclassified violations of state law or local ordinance punishable by fine only (including arrest reports and citations) – 6 months
  - b. Class A & B misdemeanors and state jail felonies. – 2 years
  - c. Second and third-degree felonies and Driving While Intoxicated offenses. – 10 years
  - d. First-degree and capital felonies. – 50 years e. Or, for any classification of offense. – Date of Death, if known.

#### O. ISSUES RELATED TO PRIVACY

##### 1. Privacy Considerations

The proliferation of camera phones, advances in surveillance technology and the emergence of social media have changed the way people view privacy, contributing to the sense that "everyone is filming everyone." As technology advances and expectations of privacy evolve, it is critical that as a department, we carefully consider how the technology we use affects the public's privacy rights, especially when the courts and our legislatures have not yet provided clear guidance on these issues.

BWC's raise many privacy issues that have not been considered before. Unlike many traditional surveillance methods, BWC's can simultaneously record both audio and video and capture close-up images that allow for the potential use of facial recognition technology. In addition, while stationary surveillance cameras generally cover only public spaces, BWC's give officers the ability to record inside private homes and to film sensitive situations that might emerge during calls for service.

##### 2. Recording Inside Private Homes

A citizen of the United States has no greater expectation of privacy than within the confines of their home; more specifically, within the interior walls of their home. An officer may record inside a home if they have the legal right to be there. Officers entering a home in response to a call for service, pursuant to a valid search warrant, or with consent of the resident, can record what they find inside.

### 3. Public Disclosure & Open Records

Texas Open Records laws governs when footage from BWC's is subject to release. Although this agency does believe that broad disclosure of video can promote police agency transparency and accountability, some videos -- especially recordings of victims from inside people's homes and where the possibility of nudity might exist will raise privacy concerns if they are released to the public or the news media. When determining how to respond to open records requests, we must balance the legitimate interest of openness with protecting privacy rights.

Texas law states that a law enforcement agency may NOT release any portion of a recording made in a private space, or of a recording involving the investigation of conduct that constitutes a misdemeanor punishable by fine only and does not result in an arrest, without written authorization from the person who is the subject of that portion of the recording or, if the person is deceased, from the person's authorized representative. A recording is confidential if the recording was not required to be made public by law or policy and does not relate to a law enforcement purpose.

## P. BWC's IN SCHOOLS

### 1. POLICE RESPONSE TO SCHOOLS

- a. An officer, who receives a call for service in or upon school property, shall employ the guidelines of the policy as they would for any call for service.
- b. Video of criminal activity shall be treated no differently than any other record as it relates to evidence and its retention.

## Q. LIMITATIONS OF BWC'S

1. A camera does not follow your eyes as they see.

At the current level of development, a BWC is not an eye-tracker. A BWC photographs a broad scene but it cannot document where within that scene you are looking at any given instant. If you glance away from where the camera is concentrating, you may not see action within the camera frame that appears to be occurring "right before your eyes."

In Short, there can be a huge disconnect between your field of view and your visual perception and the camera's. It must be recognized that someone reviewing what is

caught on camera and judging the actions of the officer could have a profoundly different sense of what happened.

2. Some important danger cues cannot be recorded.

Tactile cues (relating to the sense of touch) that are often important to officers in deciding to use force are difficult for cameras to capture. Resistive tension is a prime example.

You can usually tell when you touch a suspect whether they are going to resist. You may quickly apply force as a preemptive measure, but on camera it may look like you made an unprovoked attack, because the sensory cue you felt does not record visually.

It is imperative that proper explanations of the officer's action be articulated in reports to include but not limited to Use of Force Reports.

3. Camera speed differs from the speed of life.

Because BWC's record at a much higher speed than typical convenience store or correctional facility security cameras, it is less likely that important details will be lost in the millisecond gaps between frames, as sometimes happens with lesser quality devices.

But it is still theoretically possible that something as brief as a muzzle flash or the glint of a knife blade that may become a factor in a use-of force case could still fail to be recorded.

People who do not understand this reactionary process will not factor it in when viewing the footage.

4. A camera may see better than you do in low light

The high-tech imaging of BWC's allows them to record with clarity in many lowlight settings. When footage is screened later, it may be possible to see elements of the scene in sharper detail than you could at the time the camera was activated.

If an officer is receiving less visual information that the camera is recording under time-pressured circumstances, you are going to be more dependent on context and movement in assessing and reacting to a potential threat. In dim light, a suspect's posturing will likely mean more to you immediately than some object he is holding. When footage is reviewed later, it may be evident that the object in his hand was a cell phone, say, rather than a weapon. An officer under these circumstances cannot be expected to have seen that as clearly as the camera did. In retrospect, the officers' action may then seem highly inappropriate.

Therefore, it is even more important for an officer to articulate why they did what they did in writing and even when the camera is still filming. Documentation is always the key to our business.

5. Body may block the view.

How much of the scene a camera captures is entirely dependent on where it is positioned and where the action takes place. Depending on location and angle, a picture may be blocked by your own body parts, from your nose to your hands and arms.

The firing of a weapon such as a handgun, rifle, shotgun or taser for example, a camera on your chest may not record much more than your extended arms and hands. Or just blading your stance may obscure the camera's view. Critical moments within a scenario that you can see may be missed entirely by your BWC because of these dynamics, ultimately masking what a reviewer may need to see to make a fair judgment.

6. A camera only records in 2-D.

Because cameras do not record depth of field, the third dimension that is perceived by the human eye -- accurately judging distances on footage can be very difficult.

Depending on the lens involved, cameras may compress distances between objects or make them appear closer than they really are. Without a proper sense of distance, a reviewer may misinterpret the level of threat an officer was facing.

7. The absence of sophisticated timestamping may prove critical.

Timestamping is automatically imposed on camera footage down to the second. Generally, measuring the action in some high profile, controversial cases is not sophisticated enough. It may become difficult or near impossible to fully analyze and explain an officer's perceptions, reaction time, judgment and decision -- making it critical to break the action down to units of one-hundredths of a second or even less.

When reviewers see precisely how quickly suspects can move and how fast the various elements of a use-of-force event unfolds, it can radically change their perception of what happened, and the pressure involved, which the officers were under to act.

8. One camera may not be enough.



The more cameras there are recording an event the more opportunities there are to clarify uncertainties. The angle, ambient lighting and other elements will almost certainly vary from one officer's perspective to another and syncing the footage will provide broader information for understanding the dynamics of what happened. What looks like an egregious action from one angle may seem perfectly justified from another.

9. A camera encourages second-guessing.


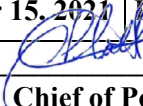
According to the U.S. Supreme Court in *Graham v. Connor*, 490 U.S. 386 (1989), an officer's decisions in tense, uncertain, and rapidly evolving situations are not to be judged with the "20/20" vision of hindsight. In the real-world aftermath of an event, camera footage provides an almost irresistible temptation for reviewers to play the "coulda-shoulda" game.

Therefore, as part of the incident investigation, this policy, along with state law, recommends and allows an officer to see what his/her body camera and other cameras recorded. Officers are cautioned, however, to regard the footage only as informational. Officers should not allow it to supplant their first-hand memory of the incident. Justification for an officer's action will come from what the officer reasonably perceived, not necessarily from what a camera saw.

10. A camera can never replace a thorough investigation.

A BWC's recording should never be regarded solely as the Truth about a controversial incident. It needs to be weighed and tested against witness testimony, forensics, the involved officer's statement, and other elements of a fair, thorough, and impartial investigation that takes human factors into consideration.

This is in no way intended to belittle the merits of BWC's. The limitations of BWC's and others need to be fully understood and evaluated to maximize their effectiveness and to assure they are not regarded as infallible "magic bullets" by people who do not fully grasp the realities of force dynamics.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 6.0 Use of Force</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices: 2.25, 3.01, 3.02, 3.04, 6.01, 6.02, 6.03, 6.06, 6.07, 6.08, 6.09, and 6.10.</b>	

## I. POLICY

This department values the protection and sanctity of human life. It is, therefore, the policy of this department that officers use only the force that is reasonably necessary to effectively bring an incident under control while protecting the lives of the officer and others.

The use of force can be viewed as an extension of the right to arrest. An officer's use of force must always be reasonable under the circumstances and should be no greater than the least amount of force necessary to make the arrest and/or stop violent behavior.

The officer's actions will be reviewed based upon the information known to the officer at the time the force was used. Information discovered after the fact will not be considered when assessing the reasonableness of the use of force.

Officers are prohibited from using any force as a means of punishment, in the process of an interrogation, or prohibition of law.

## II. PURPOSE

In recent years, the issue of use of force by police officers has developed into an area of paramount concern to citizens, the individual officer, and police administration.

As in all police activities, the use of force requires sound judgment on the part of the officers. The liability of officers who have failed or refused to exercise this good judgment is well documented in civil and criminal court cases against those officers. While procedures can offer guidelines, the split-second decisions and complex factors which are a part of each situation in which an officer uses force are unpredictable, making specific procedures and rules almost impossible.

This document shall approach the critical area of force by attempting to provide a direct and simple standard to rational and practical guidelines in the use of force. Generally, officers are guided by Chapter 9 Penal Code and applicable case laws, in determining use of force applications or restrictions.

This policy is for departmental use only and does not apply in any criminal or civil proceeding. This document should not be construed as a creation of a higher legal standard for safety or care in an evidentiary sense with respect to third party claims. Violations of this

order shall only form the basis for departmental administrative action. This document should also not be construed as creating a standard for the use of force higher than that created by applicable statutory or case law.

### **III. DEFINITIONS**

- A. Deadly force: Any use of force that creates a substantial risk of causing death or serious bodily injury.
- B. Non-deadly force: Any use of force other than that which is considered deadly force. Non-deadly force includes but is not limited to; handcuffing and any physical force, effort or technique used against another.
- C. Serious Bodily Injury: “Serious bodily injury” means bodily injury that creates a substantial risk of death or that causes death, serious permanent disfigurement, or protracted loss or impairment of the function of any bodily member or organ.
- D. Objectively reasonable:
  - 1. This term means that, in determining the necessity for force and the appropriate level of force, officers shall evaluate each situation in light of the known circumstances, including, but not limited to, the seriousness of the crime, the level of threat or resistance presented by the subject, and the danger to themselves and the community.
  - 2. In evaluating the reasonable application of force, officers may consider their own age, size, strength, skill level with department weapons, state of health, and the number of officers opposing the number of suspects.

### **IV. PROCEDURES**

- A. Use of non-deadly force
  - 1. Where deadly force is not authorized, officers may use only that level of force that is objectively reasonable and necessary to bring an incident under control. (TEXAS BEST PRACTICES: 6.01)
  - 2. Officers are authorized to use department-approved, non-deadly force techniques and issued equipment when one or more of the following apply:
    - a. To protect the officer or others from physical harm.
    - b. To restrain or arrest an individual who is resisting a lawful arrest or detention.
    - c. To bring an unlawful situation safely and effectively under control.
- B. Use of deadly force
  - 1. Law enforcement officers are authorized to use deadly force when one or both of the following apply:

- a. To protect the officer or others from what is reasonably believed to be an immediate threat of death or serious bodily harm. (TEXAS BEST PRACTICES: 6.02)
- b. To prevent the escape of a fleeing violent felon whom the officer has probable cause to believe will pose a significant threat of death or serious physical injury to the officer or others.
- c. Where practicable, prior to discharge of the firearm, officers shall identify themselves as law enforcement officers and state their intent to shoot.

#### C. Deadly Force Restrictions

1. Warning shots are prohibited and shall not be fired. (TEXAS BEST PRACTICES: 6.09).
2. Firearms shall not be discharged at or from a moving vehicle, attempting to disable the vehicle.
3. Officers threatened by an oncoming vehicle shall make a reasonable effort to attempt to move out of its path, if possible, instead of discharging a firearm at it or any of its occupants. However, if an officer reasonably believes that a person is immediately threatening the officer or another person with deadly force by means of a vehicle, an officer may use deadly force against the driver of the vehicle.
4. Officers may use deadly force to destroy an animal that represents a threat to public safety or as a humanitarian measure if the animal is seriously injured and the officer reasonably believes that deadly force can be used without harm to the officer or others. In these circumstances, a supervisor shall be contacted prior to the use of deadly force if time permits and a report of the incident made.

### V. LIMITATIONS ON FORCE

#### A. The following acts associated with the use of force are prohibited:

1. Application of a choke hold or carotid control holds, except when the officer reasonably believes such holds are the only means of protecting himself/herself or another person from an imminent threat of serious physical injury or death and the use of deadly force would be authorized.
2. Use of flashlights as batons. An officer may use a flashlight or other object designed for a use other than as a weapon only to defend himself or herself or another from imminent serious bodily injury or death and then only if departmentally sanctioned methods are not available or are impractical. The use of a flashlight or other alternative weapon under such circumstances, depending on the manner of use, may be deemed an application of deadly force.

## VI. Dynamic Resistance Response Model

Law enforcement agencies typically examine traditional use of force models for guidance in establishing their policies. Unfortunately, models employed today contain complicated language and distort the state of the law by placing the focus on the officer's actions and minimizing those of the individual initiating the resistance. Such emphasis may mislead citizens and those in the judicial system into analyzing why all possible lesser force options were not used, causing concern for officers, departments, and the public. Citizens should respect the authority and lawful commands of police officers, but, sadly, some choose to resist, forcing contacts to unnecessarily escalate into physical confrontations.

Long before the changes brought about by *Tennessee v Garner*<sup>1</sup>, which crafted a new constitutional framework for the proper use of force, the U.S. Supreme Court established a history of reasonableness that guided officer conduct and offered an understanding of the difficulties and complications inherent in the profession. Accordingly, the Court has provided the law enforcement community with a wide path to tread while carrying out its mission. Within the constitutional parameters established by the Court, most agencies require officers to adhere to more restrictive use of force policies, which, in fact, have not entirely eliminated the controversy surrounding officer-citizen encounters as evidenced by continued allegations of misuse of force. Policies often are created or expanded under intense political and public relations pressures that overwhelm the proper channels of policy formulation.

Many departments have faced civil suits for the alleged misuse of emerging less-lethal equipment. Others have responded by prohibiting the use of these tools on suspects outside specific age parameters or on those who suffer from specific medical conditions. This places an officer in an untenable position - if the officer misjudges a suspect's age or fails to accurately determine a medical condition, the officer may be placed outside of policy, focusing intense scrutiny on the officer and the department. A common result of overly restrictive policies is an increasing reluctance to use practical law enforcement tools developed specifically to increase the safety of both citizens and officers.

Improper use of force by a few officers should not cause an automatic policy change affecting an entire agency. Before adopting a more restrictive policy, departments should consider possible ramifications of changes, such as the impact on morale, an increased need for training, the effect on future litigation, and possible confusion among officers.

The solution for law enforcement agencies does not involve removing options nor adopting additional policies and restrictions. Rather, a new approach that more accurately reflects the intent of the law and the changing expectations of society can help address these issues. To this end, the Dynamic Resistance Response Model (DRRM) will be utilized as the use of force continuum employed by Teague Police Department.

DRRM is a new approach that more accurately reflects the intent of the law and the changing expectations of society. When officers clearly understand a reasonable use of force model, they are better prepared to make appropriate use of force decisions. Officers faced with potentially life-threatening situations need simple, clear, unambiguous, and consistent

guidelines regarding use of force. To this end, the Dynamic Resistance-Response Model (DRRM) combines a use-of-force continuum with an application of four broad categories of suspects.

Dynamic indicates that the model is fluid. Suspects can move rapidly from one level of resistance to the next. The public must realize that situations can quickly and dangerously transition from one category to another. Officers should never assume a suspect currently complying will continue to do so. Officers should always be prepared for an attack no matter how compliant an individual initially appears.

Resistance demonstrates that the suspect controls the interaction. A major failing among current Use of Force models is the emphasis on the officer and the amount of force used. This places officers in a weak position during accusations of excessive force as the focus is on the officer's actions, rather than on the suspect's. The DRRM emphasizes that the suspect's level of resistance determines the officer's response and delineates suspects into one of four categories: **not resistant** (compliant), **passively resistant**, **aggressively resistant**, and **deadly resistant**.

#### A. Not Resistant

Suspects who do not resist but follow all commands are compliant. Only a law enforcement officer's presence and verbal commands are required when dealing with these individuals; no coercive physical contact is necessary.

#### B. Passively Resistant

A passively resistant suspect fails to follow commands and may be verbally abusive. He may attempt to move away from the officer, escape from the officer's grip, or flee. The suspect's actions are neutral or defensive, and the officer does not feel threatened by his actions. Appropriate responses include using a firm grip, control holds, and pressure points to obtain compliance.

#### C. Aggressively Resistant

An aggressively resistant suspect takes offensive action by attempting to push, throw, strike, tackle, or physically harm the officer or another person. To defend himself, the officer must respond with appropriate force to stop the attack. The officer feels threatened by the suspect's actions. Justified responses include the use of personal weapons (hands, fists, feet), batons, pepper spray, and an ECD.

#### D. Deadly Resistant

A deadly resistant suspect will seriously injure or kill the officer or another person if immediate action is not taken to stop the threat. The officer is justified in using force, including deadly force, reasonably necessary to overcome the offender and effect custody.

## E. APPLICATION

In the DRM diagram, no resistance (compliance) is in the center of the triangle, emphasizing that as the goal of every encounter. If a suspect's resistance level places him on one of the three corners of the triangle, the officer's response (appropriate use of force) is intended to move the suspect's behavior to the center of the triangle and compliance. If force is used by the officer in response to the suspect's resistance level, the sole purpose of the application of force is to gain compliance.

For each of the four suspect categories, officers have all the tools in the preceding categories available. In each instance, officers constantly should give commands to the suspect when doing so does not jeopardize safety.



DRRM / Diagram

## VI. DUTY TO INTERVENE AND REPORT (Texas Best Practices: 2.25)

Excessive force by any police officer or employee is untenable and will not be condoned or tolerated.

- A. All officers and employees, regardless of rank, tenure, or level of training, has a duty and responsibility to intervene in any other officer's or employee's use of excessive force.
- B. Each employee with this department, regardless of status, has an affirmative duty and responsibility to intervene and stop any other employee's use of force that clearly exceeds agency directives and training regarding what is objectively reasonable under the circumstances.
- C. Each employee, regardless of status, has a duty to immediately report, in writing, any use of excessive force to any supervisor not immediately involved in the situation.

- D. This directive will be included in the annual Use of Force training.
- E. This directive applies to both sworn and non-sworn employees.
- F. Any reports made under this section shall be investigated pursuant section IX. Department Review and Chapter 2.3 Internal Investigations.

## **VII. TRAINING**

- A. All officers shall receive training in the use of their firearms and all non-lethal weapons authorized by the department, hands-on arrest and defensive tactics, as well as the “Use of Force” policy prior to performing any law enforcement duties.
- B. All officers shall be trained and qualified with their firearms at least annually. (TEXAS BEST PRACTICES: 3.01, 3.02).
- C. All officers shall receive training in the department’s “Use of Force” policy at least annually. (TEXAS BEST PRACTICES: 3.02).
- D. All officers shall receive hands-on arrest and defensive tactics training at least every two years. (TEXAS BEST PRACTICES: 3.06).
- E. Officers shall receive training in all non-lethal weapons issued or used by the department and demonstrate proficiency with those weapons at least every two years. (TEXAS BEST PRACTICES: 3.04).
- F. All use-of-force training shall, at a minimum, comply with the standards established by TCOLE.

## **VIII. REPORTING USE OF FORCE (TEXAS BEST PRACTICES: 6.03, 6.06)**

- A. Officers shall document any application of force except for those arising in training, departmental demonstrations, or off-duty recreational activities. The documentation of use of force shall be on the form prescribed by the Chief of Police.
- B. If officers have employed any use of physical force (other than the routine use of handcuffs or use of a firm grip to direct the movements of a subject) or used any impact, electrical, or chemical weapons, or pointed or discharged any firearm, they shall first provide for appropriate medical aid for the subject (TEXAS BEST PRACTICES: 6.07) and then they will do the following:
  - 1. Immediately notify the on-duty supervisor or the Chief of Police (if the on-duty supervisor is unavailable) of any use of force or discharge of a weapon. The supervisor or Chief of Police shall determine if an immediate investigation is required. The Chief of Police should be notified immediately in any situation where deadly force is utilized or serious bodily injury results from the use of force by an officer of this department.



2. Photographs of the person, subject of the use of force, will be taken as soon as possible after the use of force to document any injury or lack of injury.
3. Submit a use-of-force form to the Chief of Police, through the chain of command, prior to the end of shift describing the incident, the force used, and any medical aid rendered. The use of force form shall be in addition to any other required reports.

## **IX. DEPARTMENTAL REVIEW**

### **A. Annual Review**


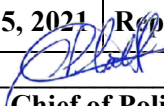
1. The officer's supervisors and the Chief of Police shall review all reported uses of force to determine the following:
  - a. If departmental policy were violated.
  - b. If the relevant departmental policy was clearly understandable and effective enough to cover the situation.
  - c. If departmental training was adequate.
  - d. If departmental equipment operated properly.
2. At least annually, the Chief of Police shall conduct an analysis of use-of force incidents and determine if additional training, equipment, or policy modifications may be necessary. (TEXAS BEST PRACTICES: 6.10.)
3. The department shall comply with all state mandated reporting requirements.

### **B. Internal Investigations**

1. An internal investigation will be conducted on any firearms discharge (other than training), and any other use of deadly force or use of force resulting in serious bodily injury by any member of the department. An internal investigation may be conducted on other use- of- force incidents. In addition to the internal investigation, a criminal investigation shall also be conducted of any incident involving the discharge of firearms or any other use of force incident where an officer or other person is injured or killed and in any other circumstances where a violation of law is suspected. The criminal investigation may be conducted by another law-enforcement agency with concurrent jurisdiction, and the results may be presented to the grand jury for review. The results of either internal or criminal investigation shall be submitted to the office of the District Attorney for review.
2. Procedures for officer-involved-shooting investigations are covered in Policy 6.3.

### C. Assignment

1. Pending administrative review, any officer whose actions have resulted in the death or serious bodily injury of another person, either through the intentional use of force or by accident involving a use-of-force weapon or action or a vehicle accident, shall be removed from line-duty assignment. This action protects the interests of both the officer and the community until the situation is resolved. This re-assignment is not considered punitive in nature. (TEXAS BEST PRACTICES: 6.08)

	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 6.1 Firearms and Qualification</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____ <div style="text-align: center;">   <b>Chief of Police</b> </div>
	<b>Reference:</b> Texas Best Practices 3.01, 3.02, 3.03, and 6.04.

## I. POLICY

The department's policy is to ensure that members are properly trained not only in the use of appropriate firearms and the circumstances of their use, but also in their safety and maintenance, regarding both on and off-duty weapons. Supervisors and the department armorer shall rigorously enforce departmental firearms standards. All personnel shall qualify at least annually with his or her sidearm and with any other firearm used or carried either on-duty or off-duty.

## II. PURPOSE

The purpose of this policy is to establish policy and procedures governing the care and maintenance of issued weapons and ammunition, the selection and use of holsters, off-duty weapons, firearms training, and qualification.

## III. PROCEDURES

### A. Authority

1. Sworn police officers who have the authority to make arrests and maintain the peace, are authorized to carry and use firearms as necessary in the performance of their duty, subject to the restrictions and guidelines of this order, the department's use-of-force policy, and state and federal law.
2. Off-duty, sworn officers of this department are encouraged to carry firearms, subject to the guidelines of this order, to protect themselves or others from imminent death or serious bodily injury in the event they must intervene in an incident off-duty before the arrival of on-duty officers.

### B. On-Duty Weapons (Handgun), Issuance and Use (TEXAS BEST PRACTICES: 6.04)

1. Only weapons issued by the department or approved by the Chief of Police will be carried or used while on-duty. The department currently issues the Glock model 45, chambered in 9 mm, as the standard handgun duty firearm for officers.
2. The departmental armorer or firearms instructor shall issue departmental weapons to authorized personnel.

3. Department firearms and ammunition are determined by the Chief of Police based on the needs of the agency.

#### C. Shotguns

1. Shotguns are assigned to patrol cars and individual officers as appropriate.
  - a. All shotguns, if issued, shall be carried with the magazine fully loaded with approved ammunition, chamber empty, trigger released, and safety off.
  - b. A minimum of five extra rounds of approved ammunition may be carried with each shotgun.
  - c. All shotguns left at the police department shall be unloaded, with chamber open and stored in gun vault or other designated location.

#### D. Patrol Rifles

Patrol rifles, the AR-15, may be issued or used by officers and supervisors who have received appropriate training and have maintained their required qualifications.

#### E. Precision Rifles

The Precision Rifle is a designed for observer/sniper missions. It serves to fulfil the tactical need for long range surveillance, effective anti-personnel or anti-materiel operations with high hit efficiency. The modern precision rifle is a portable shoulder-fired weapon system with a choice between bolt-action or semi-automatic action, fitted with a telescopic sight for extreme accuracy and chambered for a high-performance centerfire cartridge. Members of this department utilizing this weapon system will be appropriately trained and maintain their required qualifications.

#### F. Off-duty and/or secondary weapons

1. Off-duty and/or secondary weapons, either revolvers or semi-automatic pistols, and their ammunition, are purchased at the officer's expense. The armorer shall inspect and certify the off-duty or secondary weapon before it may be carried. Off-duty and/or secondary weapons must be approved by the Chief of Police, before being carried.
  - a. Officers using off-duty or secondary weapons shall qualify with the off-duty or secondary weapons during annual qualification.
  - b. The Chief of Police (or designee) shall approve any concealed holster for an off-duty or secondary weapon.
  - c. A record of all holsters and weapons used by each officer shall be maintained in their departmental file.
2. While off duty, officers may carry either an issued weapon or one purchased at officer expense, subject to the terms of this policy.

3. Officers should not carry weapons when it is inappropriate to do so, e.g. Federal Court or on Federal Property.
4. Officers will not carry weapons when consuming alcoholic beverages or prescription drugs affecting fine motor skills.
5. Off-duty weapons shall be carried safely and concealed from public view.
6. Officers shall carry the departmental badge and identification any time that they are carrying an off-duty weapon.

G. Departmental Ammunition (TEXAS BEST PRACTICES: 6.04)

1. Only factory manufactured ammunition will be used in departmental personal weapons for on-duty or off-duty use. The department will select and purchase on-duty ammunition for each qualification and old ammunition will be fired during qualification to ensure fresh ammunition is carried in on-duty firearms.
2. Officers are responsible for the purchase of ammunition for their off-duty weapon. Ammunition should be factory manufactured.
3. Only factory manufactured 00 Buck and slug rounds will be used in departmental shotguns.
4. Only factory manufactured .223/5.56, 55-gram soft-point ammunition will be used in departmental patrol rifles, unless otherwise authorized by the Chief of Police.
5. Only factory manufactured match grade ammunition will be used in departmental precision rifles, unless otherwise authorized by the Chief of Police.

H. Security of weapons

1. Officers are responsible for the care, cleaning, and security of departmental weapons issued to them, whether on-duty or off-duty.
2. Officers shall report any weapon malfunction to the Chief of Police via the chain of command.
3. Officers are responsible for the safe and secure storage of issued weapons when off-duty in a manner that prevents theft or unauthorized access or use.

I. Department Firearms Proficiency Officer and Armorer

1. The Chief of Police may appoint at least one sworn member of the department to be the departmental firearms proficiency officer and armorer. The armorer shall be a firearms instructor certified by the Texas Commission on Law Enforcement.

2. Their duties are as follows:
  - a. Schedule, supervise, and maintain records on all firearms qualifications required by the department.
  - b. Maintain non-issued departmental weapons and associated equipment.
  - c. Inspect all weapons being returned to the armory to ensure they are clean and serviceable.
  - d. Repair or submit to a qualified gunsmith for repair all departmentally owned malfunctioning weapons, as authorized by the Chief of Police.
  - e. Maintain records of issuance, care, and maintenance of departmental and personally owned weapons and associated items used on-duty.
  - f. Issue departmental ammunition.
  - g. Annually inspect and certify as serviceable both departmental and personally owned firearms that are authorized for on-duty and off-duty use.
  - h. Inspect and authorize the use of holsters for off-duty use and for on-duty use if the officer prefers to use a holster other than one issued by the department.
3. The armorer shall maintain a record that includes identification of all firearms that have been certified as safe, and identification of those officers who have qualified with each of the firearms. This record shall include the following:
  - a. Officer's name and badge or employee number.
  - b. Make and model of weapon.
  - c. Serial number of the weapon.

J. Modification of weapons.

Departmental weapons shall not be modified or altered without the written approval of the Chief of Police except as outlined below.

1. Substitution of grips
  - a. Grips shall be of high-quality wood, rubber, or polyurethane.
  - b. Grips shall be the color of the natural wood, or plain black or brown.
  - c. Target-style grips, or any grips that interfere with the operation of the weapon, are not authorized.

2. Modification of privately owned weapons designated by officers as duty weapons.
  - a. Substitution of grips as outlined in 1.b above is authorized.
  - b. Trigger shoes are prohibited. (A trigger shoe is a block of metal configured to fit snugly on the front face of the trigger of a designated firearm, often utilized in competition weapons)

#### K. Firearms inspections

1. Annually, either the firearms instructor or the armorer shall thoroughly inspect each weapon during qualification on the range. Documentation of this inspection will be maintained by the Chief of Police on the annual firearms qualification report, which will be kept in the officer's TCOLE file. (TEXAS BEST PRACTICES: 3.03)
2. On a monthly basis, supervisors shall inspect subordinate officers' issued firearms to ensure that they are maintained in a clean and serviceable condition.
  - a. Firearms inspections shall include side arms, shotguns, authorized rifles, ammunition pouches, and holsters.
  - b. Ammunition shall be inspected to ensure that it is of departmental issue, of correct quantity, and in serviceable condition.
  - c. Upon completion of monthly inspections, the supervisor shall forward a memorandum to the Chief of Police that documents the following information:
    - i. The date the inspection was held.
    - ii. The name of each officer inspected.
    - iii. The findings of the inspection.

### IV. PROCEDURES FOR QUALIFICATION

#### A. Qualification rules

1. Officers must qualify at least annually with any weapon they carry or use on/off duty, or as a back-up system, or when they change weapons. (TEXAS BEST PRACTICES: 3.01)
2. The firearms instructor or armorer shall always be in charge when officers are on the firing range for qualification, no matter their ranking in the department.
3. Officers using departmentally issued weapons must qualify with ammunition issued by the department.
4. Every officer shall fire the regular firearms course approved by the Texas Commission on Law Enforcement.

5. Officers who fail to qualify on their first attempt shall immediately attempt qualification a second time. Officers who fail to qualify on the second attempt shall be placed in remedial training as soon as practicable and shall be removed from patrol or investigative duties until the standards expressed herein are met. Officers who cannot qualify within fifteen days of the original qualification shall be subject to termination. (TEXAS BEST PRACTICES: 3.01)
6. The armorer will maintain records of each officer's firearms qualifications including:
  - a. The officer's name and badge or employee number
  - b. The date of qualification
  - c. The weapons(s) used during qualification
  - d. A description of the course of fire and notation of pass/fail.
7. The armorer or firearms instructor shall inspect all weapons before firing to (1) ascertain that the weapons are safe and (2) to ensure that the weapons have been properly maintained.

#### B. Shotgun

1. Every officer must pass the shotgun qualification course, whether carrying a department-issued shotgun or not.
2. The qualification course shall include the following:
  - a. Knowing how to load and unload the shotgun combat style.
  - b. Firing at least 10 shots, not all from the same position.
3. Officers shall qualify with the shotgun at least annually.

#### C. Patrol Rifle

Officers who are trained and authorized to use the patrol rifles must qualify at least annually with the rifle on a TCOLE approved course of fire.

#### D. Precision Rifle


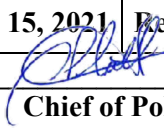
Officers who are trained and authorized to use the precision rifle must qualify at least annually with the rifle on a TCOLE approved course of fire.

#### E. Firearms and Use of Force Instruction

1. All department personnel whose duties require the carrying of firearms shall receive familiarization instruction on their firearms before range qualification.



2. At least annually, personnel whose duties require the carrying of firearms shall receive training in the mechanics of the weapon (stripping, lubricating, nomenclature, troubleshooting, and misfires), and sound safety practices.
3. At least annually and in connection with firearms training, personnel whose duties require the carrying of firearms will receive training in the department's use-of-force policy. (TEXAS BEST PRACTICES: 3.01)
4. Use-of-force and use-of-deadly force training will be conducted at least annually in conjunction with firearms use and firearms qualification. (TEXAS BEST PRACTICES: 3.02)

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 6.2 Less-than-Lethal Weapons</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 3.04	

## I. POLICY

In the interest of public safety, the department provides officers with a range of less-than-lethal options. The department's policy intends to ensure that officers are properly trained in the use of non-lethal and less-than-lethal weapons, and that they will adhere to the department's policy for the circumstances of their use. Supervisors shall rigorously enforce departmental weapons standards.

All sworn personnel shall qualify at least annually with departmental non-lethal and less-than-lethal weapons. Officers shall not carry or use any non-lethal or less-than-lethal weapon if they have not received training and been qualified. Officers will carry only those non-lethal and less-than-lethal weapons that have been approved by the department. (TEXAS BEST PRACTICES: 3.04)

## II. PURPOSE

The purpose of this policy is to establish procedures governing the issuance, training, care and maintenance, and proper use of non-lethal and less-than-lethal weapons as well as the standards that officers must meet to qualify for carrying and using such weapons.

## III. GENERAL PROCEWURES

### A. Approved Weapons

1. Non-lethal and less-than-lethal weapons currently approved by the department include:
  - a. ASP Baton (departmental issue)
  - b. OC Pepper Spray (departmental issue)
  - c. Conducted Energy Weapon (CEW) (departmental issue)

2. Based on the needs of the agency, the Chief of Police determines which non-lethal or less-than-lethal weapons will be used by the department. If such weapons are added to the department a policy revision will be completed and published and disseminated to all officers. Training and qualification will be required before any use or deployment of new weapon systems.
3. Officers will not carry or use any weapon that has not been approved by the Chief of Police.
4. Officers will not carry or use any weapon that they have not been trained or qualified for by the department.

#### B. Security of weapons

1. Officers are responsible for the care and security of departmental weapons issued to them.
2. Officers shall make a written report of any weapon loss or malfunction to the Chief of Police via the chain of command.
3. Officers shall not use a weapon after it has malfunctioned until it has been repaired and approved for use by an authorized person.

#### C. Modification and maintenance of weapons

1. Departmental weapons shall not be modified or altered without written approval of the Chief of Police.
2. Any modification or alteration shall be in accordance with the manufacturer's recommendation.
3. Officers are responsible for cleaning and maintenance of the non-lethal or less-than-lethal weapons issued to them.
4. All non-lethal or less-than-lethal weapons shall be plainly distinguishable from lethal weapons.

#### D. Weapon inspections

1. Officers shall inspect issued weapons at the beginning of each duty assignment to ensure that they are in proper working order.
2. Supervisors shall inspect issued weapons at least monthly and shall document the inspections in a memorandum to the Chief of Police indicating which officers' weapons were inspected and the results of the inspection.
3. Weapons that fail inspection shall be returned to the armorer and not reissued to the officer until repairs are made.

## **IV. QUALIFICATION REQUIREMENTS**

### **A. Required instruction and qualification**

1. All department personnel shall receive training with any non-lethal and less-than-lethal weapons that they will carry.
2. Training shall cover the mechanics of the weapon, sound safety practices, and departmental policy governing the use of the weapon and the use-of-force.
3. Tactical considerations shall be a part of this training.
4. Officers will receive training and demonstrate proficiency (qualify) at least annually on all departmental non-lethal or less-than-lethal weapons systems. Failure to qualify with a non-lethal or less-than-lethal weapons will be cause for remedial training. The officer will not carry or utilize the non-qualifying weapon until properly trained and qualified. (TEXAS BEST PRACTICES: 3.04)
5. Instructors for any non-lethal or less-than-lethal weapon where the manufacturer recommends the instructors be certified before providing initial or refresher training shall be certified before providing the said training. (TEXAS BEST PRACTICES: 3.04)

### **B. Qualification rules**

1. The firearms instructor or armorer shall always be in charge when officers are qualifying with non-lethal or less-than-lethal weapons.
2. The Chief of Police will maintain records, prepared by the firearms instructor or armorer, of each officer's qualifications with non-lethal and less-than-lethal weapons including:
  - a. The officer's name and badge or employee number,
  - b. The date of qualification and the name of the weapon system.

## **V. ASP BATON**

- A. The department authorizes the carrying and use of the ASP baton as the only striking weapon for officers. All other forms of striking or punching weapons are prohibited, including but not limited to saps, blackjacks, brass knuckles, slapjacks, nunchaku, and similar sticks.
- B. Flashlights carried by officers are not to be used as striking instruments, unless and to the degree that, the officer reasonably believes its use is immediately necessary to protect the officer or another from injury.

- C. Officers who carry the ASP shall be trained and demonstrate proficiency in its use. The weapon may be used in quelling confrontations involving physical violence where higher levels of force are unnecessary or inappropriate and lesser levels are inappropriate or ineffective.
  - 1. The ASP should not be used to strike handcuffed individuals or to threaten or intimidate people.
  - 2. Officers shall not raise the ASP above the head to strike a blow to a person's head.
- D. All uses of the ASP baton will be immediately reported to a supervisor and documented in an incident report, which is to be forwarded to the Chief of Police, as well as a use-of-force report.

## **VI. OC PEPPER SPRAY**

### **A. Authorization**

- 1. Only officers who have completed the prescribed course of instruction on the use of OC are authorized to carry the device.
- 2. Officers whose normal duties/assignments may require them to make arrests or supervise arrestees shall be required to qualify for and to carry departmentally authorized OC Pepper Spray while on duty.

### **B. Uniformed officers shall carry only departmentally authorized OC canisters in the prescribed manner on the duty belt. Non-uniformed officers may carry OC in alternative devices as authorized by the Chief of Police.**

### **C. Usage Criteria**

- 1. OC spray is considered a “use of force” and shall be employed in a manner consistent with this agency’s use-of-force policy.
- 2. OC may be used in the following circumstances:
  - a. When verbal dialogue has failed to bring about the subject’s compliance.
  - b. When the subject is physically resisting or has signaled his/her intention to physically resist the officer’s efforts to make the arrest.
  - c. Verbal resistance is not justification for use of OC spray. Verbal resistance, coupled with other mitigating factors, may be justification for use of OC Spray.

3. Whenever practical and reasonable, officers should issue a verbal warning prior to using OC against a suspect.
4. Once a suspect is incapacitated or restrained, use of OC is no longer justified.
5. Officers shall summon medical assistance after deployment of OC spray.

#### D. Usage Procedures

1. Whenever possible, officers should be upwind from the suspect before using OC and should avoid entering the spray area.
2. An officer should maintain a safe distance from the suspect, which is between 2 and 10 feet, depending on the circumstances.
3. A single spray burst of between one and three seconds should be directed at the suspect's eyes, nose, and mouth. Additional burst(s) may be used if the initial or subsequent burst proves ineffective.
4. Use of OC should be avoided, if possible, under conditions where it may affect innocent bystanders, other officers, or contaminate a public facility.

#### E. Effects of OC and Officer Response

1. Within several seconds of being sprayed by OC, a person will normally display symptoms of temporary blindness, have difficulty breathing, burning sensation in the throat, nausea, lung pain, and/or impaired thought processes.
2. The effects of OC vary among individuals. Therefore, all persons shall be handcuffed as soon as possible after being sprayed.
3. Officers should also be prepared to employ other means to control the person—to include, if necessary, other force options consistent with agency policy—if the person does not respond sufficiently to the spray and cannot otherwise be subdued.
4. Immediately after spraying a person, officers shall immediately summon emergency medical aid to provide medical treatment to a person affected by the spray.
5. Persons who have been sprayed shall be monitored continuously for indications of medical problems and shall not be left alone while in police custody.
6. Officers should provide assurance to persons who have been sprayed that the effects are temporary and encourage them to relax.

7. Air will normally begin reducing the effects of OC spray within 15 minutes of exposure. However, once the person has been restrained, officers shall assist him by rinsing and drying the exposed area.
8. Assistance shall be offered to any individuals accidentally exposed to OC spray who feel the effects of the agent.

#### F. Reporting Procedures

1. Accidental discharges as well as intentional uses of OC spray against an individual in an enforcement capacity shall be reported to the officer's immediate supervisor as soon as possible.
2. A use-of-force report shall be completed following all discharges of OC spray except during testing, training, malfunction, or accidental discharge.

#### G. Replacement

1. All OC spray devices shall be maintained in an operational and charged state by assigned personnel.
2. Replacements for damaged, inoperable, or empty devices are the responsibility of officers to whom they are issued.
3. Replacements of OC spray canisters shall occur when the canister is less than half full, which can be determined by weighing the canister.
4. OC canisters shall be inspected and weighed at the firing range during firearms qualification. A record of the results of this inspection and weighing shall be maintained by the appropriate agency authority.
5. Unexplained depletion of OC from any canister issued to an officer shall require an investigation and written report by the officer's supervisor to the commanding officer.

## VII. CONDUCTED ENERGY WEAPON

### A. Conducted Energy WEAPON

1. A conducted energy weapon (CEW) is used to electrically disrupt neuro and muscular control. It allows officers to quickly subdue a resisting person without having to resort to the use of deadly force.
2. As with any other weapon, precautions must be observed in the use of CEWs. Any person who has been controlled with the CEW must be monitored for any medical problems.

3. The duties of supervisors of officers issued the CEW include active supervision, maintaining managerial controls, and ensuring that officers are following this order.

#### B. Training and Qualification Procedures

1. Only personnel who successfully complete the department's approved training course and demonstrate the required proficiency in the use of the CEW shall be certified and allowed to carry the CEW.
2. All training and qualification for the CEW shall be conducted by certified instructors.
3. It shall be the responsibility of the CEW instructor to train and certify all eligible officers on the proper techniques for using the CEW.
4. The CEW instructor shall be responsible for compiling and analyzing data from incidents involving the use of the CEW to identify training related needs and issues.
5. To maintain proficiency in the use of the CEW, all officers certified to carry the weapon shall receive mandatory in-service training at least annually.

#### C. Carrying the CEW

1. Certified officers shall carry the CEW on their duty belts.
2. The CEW shall never be left unsecured.
3. Only holsters approved by the training unit will be utilized.
4. The CEW shall always be carried on the side opposite the duty handgun, in a cross-draw manner.
5. Personnel issued the CEW shall be responsible for the proper maintenance and care of the weapon. This shall include periodically checking battery life and the expiration date of air cartridges and wiping away dirt and dust.
6. Officers authorized to carry the CEW will conduct a spark check at the beginning of every shift. This will ensure the capacitor is properly charged and ready for deployment, should the need arise.

#### D. Authorized Use of the CEW

1. The CEW may be utilized in situations when necessary to subdue a noncompliant person when lesser means of control have not been successful, and the suspect is *physically* resisting officers.
2. The act of verbal non-compliance shall not justify the use of the CEW weapon.



3. The CEW may be utilized to debilitate a person who poses an immediate threat of bodily injury, serious bodily injury, or death to himself/herself, the officer, or others.

E. Prohibited Use. Use of the CEW is strictly prohibited under the following circumstances.

1. When flammable gases or liquids are known to be near the subject.
2. One at a time: No more than one officer at a time should activate a CEW against any person.
3. Where the suspect is at an elevated location and there exists risk of serious injury or death from a fall. This includes proximity to deep water or other similar locations.
4. Extra caution should be taken regarding CEW usage on higher risk populations unless the situation would justify a high level of force, including deadly force, and the use of the CEW is an effort to avoid using the higher level of force. Higher risk populations refer to visibly pregnant females; young children; the visibly frail or infirm; elderly (over 65); those who appear to weigh less than 100 pounds. (This requirement is promulgated out of an abundance of caution as there is no scientific evidence to suggest that higher risk populations have been clinically established to be at greater risk from CEW deployment than the general population.).
5. Handcuffed prisoners, without the expressed authority of a supervisor. Exigent circumstances must exist, such as to prevent the subject from injuring himself or others and other means of control are ineffective or unavailable.
6. On a subject who is confined to a wheelchair unless it is objectively clear that CEW is needed to prevent serious injury to the individual and/or if deadly force is justified.
7. On a subject in control of a vehicle.
8. On individuals with known neuromuscular disorders, such as muscular sclerosis, muscular dystrophy, or epilepsy.
9. Caution should be used on persons known to be wearing pacemakers or other biomedical devices sensitive to electrical current.

F. CEW Deployment

1. Prior to deploying the CEW, whenever reasonable and practical, verbal warnings shall be issued to the subject, which will allow the subject the opportunity to comply with the officer's commands.
2. In situations where CEW use is a possibility, officers should consider requesting emergency medical services be dispatched for standby before use.

3. Prior to deploying the CEW, the deploying officer shall announce the word “CEW” or “Taser” (a verbal notification consistent with the training received by the officer deploying the weapon) to alert others of the impending use of the weapon.
4. “Clear” shall be announced by the deploying officer after using the CEW and prior to affecting the arrest, to alert others that the weapon is no longer being deployed.
5. When activating a CEW, the officers should use it for one standard cycle and stop to evaluate the situation. (A standard cycle is five seconds.) If subsequent cycles are necessary, only the number and duration of cycles necessary to place the subject in custody will be used. Officers shall justify in their report each use of the CEW cycle, as each cycle is a separate and distinct use of force.
6. Officers should consider that CEW exposure lasting longer than 15 seconds (whether due to continuous or multiple cycles) may increase risk of death or serious bodily injury.
7. Applications of more than 15 seconds should be weighed against other force options.
8. Officers will be particularly alert for medical distress of the subject.
9. Officers should make every effort to avoid firing darts or directing the contact stun method at a subject's head, neck, front chest area, or genitalia. Preferred targeting is the center mass of the subject's back. Where back targeting is not possible, officers should avoid chest shots, as prescribed in current training guidelines.
10. The CEW direct contact stun method may be utilized as an alternative deployment method when both probes fail to make contact with the subject and its effectiveness is reduced or the regular deployment method is either not possible or likely to be ineffective.
11. The CEW shall not be used in any manner that constitutes torture, torment, or punishment.
12. It shall not be used to elicit statements, awaken an intoxicated subject, or punish any individual.

#### G. Post Deployment

1. **Immediate Restraint:** The person will be restrained immediately to prevent additional resistance or injury. The person will not be restrained in a manner that impairs respiration. If other restraints are unavailable, the person may be handcuffed in front using a belt or strap to secure the cuffs to the body.

2. Medical Monitoring. Emergency medical services (EMS) shall be requested to respond to all instances where the CEW has been deployed. The requesting officer shall monitor the subject until EMS personnel have arrived.
3. Supervisor Response. The on-duty supervisor or Chief of Police will immediately respond to the scene of any CEW use. The supervisor will review the circumstances of the use and conduct a preliminary investigation.
4. Removal of Probes. CEW probes shall be removed as soon as possible. CEW probes that are imbedded in a subject's skin (as opposed to just clothing) shall be removed only by EMS personnel, other medical personnel, or police personnel who are trained in the removal of the probes.
5. Police personnel shall not remove CEW probes that have struck a subject's head, throat, groin, or any other sensitive area.
6. A CEW probe that has penetrated a person's skin shall be considered a biological hazard and shall be handled with the appropriate care.
7. All persons who have been subjected to a CEW activation should be monitored regularly while in police custody even if they received medical care.
8. Anyone subject to CEW deployment showing any signs of physical distress shall be transported immediately to a medical facility.

#### H. Reporting and Investigation

1. A use-of-force report shall be completed on all CEW incidents. Personnel must clearly articulate the reasons for the initial use and all subsequent cycle(s) in the use-of-force report. This includes the actual or threatened use of the CEW by an officer.
2. The supervisor responding to the scene shall conduct an immediate preliminary investigation that should include the following:
  - a. Location and interview of witnesses (including other officers).
  - b. Photographs of subject and officer injuries.
  - c. Photographs of cartridges/darts.
  - d. Collection of CEW cartridges, darts/prongs, data downloads, car video, body camera video, confetti ID tags, and copies of the device data download.

3. Photographs of the person shall be taken in all instances involving a person who is injured or complains of being injured because of the use of the CEW. Photographs should depict overall condition of the suspect, any injuries, and the locations where the probes made contact.
4. All CEW deployments or discharges, including test firings, shall be recorded in a CEW log. A supervisor must sign the CEW log verifying that the information contained therein is accurate. The CEW log is downloaded from the device.
5. Expended CEW cartridges shall be submitted as evidence. After submission, the officer shall be provided with a replacement cartridge.
6. The Chief of Police may request an outside investigation by the Texas Department of Public Safety Rangers when any of the following factors are involved:
  - a. A subject experiences death or serious injury.
  - b. A person who experiences prolonged CEW activation.
  - c. The CEW appears to have been used in a punitive or abusive manner.
  - d. There appears to be a substantial deviation from training.
  - e. A person in a high-risk population category has been subjected to activation (see list above).
  - f. Any other activation as determined by a supervisor.

#### I. Inspection

CEW instructors shall, monthly, inspect officer's CEW log to determine if there have been any discharges since the previous inspection. Any undocumented discharges shall require the officer to prepare a memorandum to the Chief of Police explaining the circumstances surrounding the discharge.


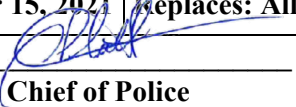
#### J. General Considerations

1. Officers should be aware that multiple activations and continuous cycling of a CEW appear to increase the risk of death or serious injury and should be avoided where practical.
2. Officers must be aware of the limitations of the CEW and be prepared to transition to other force options as needed.

3. Officers should be aware that there is a higher risk of sudden death in people under the influence of drugs and/or symptoms associated with excited delirium.
4. Officers should also be aware that CEW cartridges have experienced firing problems in extremely cold weather.
5. Officers should be aware that static electricity and radio transmissions may cause a CEW cartridge to deploy without intentional activation.

#### K. Defense Against CEW Use

1. When a person is armed with a CEW and attacks or threatens to attack a police officer, the officer may defend himself when he/she reasonably believes it is immediately necessary to avoid becoming incapacitated and risking the possibility that the subject could gain control of the officer's firearm. When possible, officers should attempt to move outside the device's range (approximately 21 feet) and seek cover, as well as request back-up officers to mitigate the danger.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 6.3 Officer Involved Shooting Investigations</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
	<b>Reference:</b>	

## I. POLICY

It is the policy of this agency that officer-involved shooting incidents be investigated with the utmost thoroughness, professionalism, and impartiality to determine if officer actions conform to the law and this agency’s policy on use of force.

## II. PURPOSE

It is the purpose of this policy to provide guidelines for the investigation of officer-involved shooting incidents and to provide guidelines to minimize the chances that involved personnel will develop or suffer from post-traumatic stress disorder.

## III. DEFINITIONS

- A. Post-Traumatic Stress Disorder: An anxiety disorder that can result from exposure to short-term severe stress, or the long-term buildup of repetitive and prolonged milder stress.
- B. Officer-Involved Shooting Incident: A line-of-duty incident where shooting causes death or serious bodily injury to an officer or other person.

## IV. PROCEDURES

- A. Officer’s responsibility when involved in a shooting incident
  - 1. Officers involved at the scene of a shooting incident shall take those measures that are reasonably possible and appropriate to protect their safety and others, and to preserve evidence essential to the investigation. This includes the following actions, undertaken in the order deemed appropriate:
    - a. Ensure that the threats to officer safety and the safety of others are over.
    - b. Notify communications of the shooting incident and request immediate assistance and notification of the Chief of Police.
    - c. Secure and separate any suspects.

- d. Relay information on any fleeing suspects to communications and other field units and work with them to establish a containment area.
  - e. Immediately request a supervisor and emergency medical services, if necessary, and any other assistance required.
  - f. If injured, administer emergency first aid to oneself first. Then administer basic first aid to suspects and others, as necessary, pending arrival of emergency medical assistance.
  - g. Holster any involved handguns or secure them in place as evidence. Secure long guns in the prescribed manner or in place as evidence.
  - h. Do not open, reload, remove shell cases or in any other manner tamper with involved firearms.
  - i. Take note of the time, survey the entire area for relevant facts, individuals who are present and who departed the scene, witnesses, potential suspects, and suspect vehicles.
2. As time and capabilities permit before supervisory and other assistance arrive:
    - a. Secure the area, establish a perimeter with crime scene tape, and limit access to those authorized persons who are necessary to investigate the shooting and assist the injured.
    - b. Protect evidence from loss, destruction, or damage that is likely to occur before backup can arrive.
    - c. Ensure that evidentiary items are not moved, or, if moved, note the original location and position of persons, weapons, and other relevant objects and evidence.
    - d. Record the names, addresses, and phone numbers of all witnesses and other persons present at the shooting scene and request that they remain on hand in order to make a brief statement whether or not they say they saw the incident.

#### B. Supervisor Responsibilities.

A supervisor shall respond as soon as possible to the scene of the incident and shall assume primary responsibility for protecting the scene and caring for involved personnel.

1. The supervisor will ensure the safety and determine the condition of the officer(s), suspect, and third parties, and summon emergency medical service providers if not yet summoned for officers, suspects, and third parties.

2. If the officer has been shot or otherwise injured, the supervisor will do the following:
  - a. Ensure that an officer accompanies and remains with the officer at the hospital.
  - b. Ensure that the officer's family is notified on a priority basis and in person when possible.
  - c. Ensure that family members are assigned transportation to the hospital or any other location where they are needed as soon as possible.
  - d. Not release the officer's name prior to the family's being notified.
  - e. Assign an officer to the family for security, support, control of the press, and visitors.
  - f. Establish communications and related matters.
  - g. Ensure that the clothing of officers and other injured persons is collected for potential evidentiary purposes.
  - h. See that related equipment of the officers is safeguarded.
3. The supervisor should contact communications and advise them of the condition of the officers and suspects and the exact location of the incident and request they immediately, if not already done, contact the following:
  - a. The Chief of Police.
  - b. Texas Rangers.
  - c. Police chaplain or advocate, if available.
4. The supervisor is to establish a command post and appoint a recorder to make a chronological record of all activities, including the names and actions of any personnel who enter the crime scene. The recorder shall prepare a supplemental report detailing his/her activities and observations. The original chronological record and the supplemental report will be placed in evidence after the scene is cleared.
5. The supervisor shall ensure that all audio/video recording systems, including in-car video systems that were at the scene at the time of the incident, are stopped and secured to protect any evidence thereon.



6. If the officer is not immediately transported to the hospital, the supervisor shall briefly meet with him/her. Only minimal, preliminary questions should be asked about the incident. The officer should be advised that a more detailed debriefing will be conducted later. The supervisor must, however, obtain sufficient information to protect the scene and begin an investigation. At a minimum the supervisor should determine the following:
  - a. If any other suspects are at large and get descriptions.
  - b. Approximate number and direction of shots fired (to protect crime scene and ensure no other persons are injured).
  - c. Description and location of any known victims or witnesses.
  - d. Description and location of any known evidence.
  - e. Any other information necessary to ensure officer and public safety and to assist in the apprehension of at-large suspects.
7. During any period where the involved officer is required to remain on the scene but has no immediate duties to fulfill, the supervisor should see that the officer is taken to a quiet area away from the scene of the incident. If available, a peer counselor or other supportive friend or officer should remain with him/her, but that person should be advised not to discuss details of the incident. At no time shall an officer be placed in the back seat of a patrol vehicle or left alone during this time.
8. The supervisor will see that a color picture of the involved officer is taken.
9. The supervisor will ensure that the overall scene and evidentiary items are photographed and videotaped.
10. The supervisor will ensure that all persons at the scene are videotaped.
11. The supervisor should advise the officer that he/she may seek legal counsel.
12. The supervisor will explain to the officer that any standard investigations concerning the incident will be discussed with the involved officers, and that the investigations shall include a criminal and an internal investigation.
13. The supervisor shall advise the officer not to discuss the incident with anyone except a personal or agency attorney, or departmental investigator until the conclusion of the preliminary investigation.
14. The supervisor will ask all officers present at the time of the incident if they are carrying any firearms other than their primary duty weapon. If so, these weapons will be examined before crime-scene personnel have left the scene.

15. The supervisor shall determine whether the circumstances of the incident require that the officer's duty weapon be taken for laboratory analysis. If the duty weapon is taken, the supervisor shall:
  - a. Take custody of the officer's weapon in a discrete manner.
  - b. Replace it with another weapon or advise the officer that it will be returned or replaced at an appropriate time.
16. The supervisor should ensure that the involved officer may notify his/her family about the incident as soon as possible. Where an officer is unable to do so, an agency official shall personally notify his family and arrange for their transportation to the hospital if needed.
17. At all times, when at the scene of the incident, the supervisor should handle the officer and all involved personnel in a manner that acknowledges the stress caused by the incident.
18. Once the scene is secure, if investigators have not yet arrived, the supervisor shall begin doing the following:
  - a. Locate and secure in place the officer's weapon and shell cases.
  - b. Locate and secure the weapons and shell cases of any suspects.
  - c. Collect information about the suspect including name, address, age, and DOB.
  - d. Locate and secure any clothing that may have been removed from the suspect or officer by medical personnel.
  - e. Attempt to determine the original shooting positions of the suspect and officer.
19. Upon arrival of investigators, the supervisor will brief the appropriate personnel on the details of the incident.
20. The supervisor shall prepare the original basic offense report concerning the incident detailing his/her activities after being notified.
21. The supervisor shall also complete a departmental use-of-force report on the incident.

C. Investigation.

This agency will request the assistance of the Texas Rangers to investigate incidents of officer-involved shootings.

This agency will conduct an administrative investigation in instances of officer-involved shootings.

1. Two different investigations may be conducted after an officer involved shooting incident.
  - a. If the officer was shot at, injured, killed, or otherwise the victim of a criminal offense, a criminal investigation will be conducted to determine the identity of the suspect and for subsequent prosecution.
  - b. If an officer shot at a suspect, an administrative investigation shall be conducted to determine compliance with departmental policy, as well as a criminal investigation to determine if the officer is criminally culpable.
  - c. If an officer shot at and hit a suspect, a criminal investigation shall be conducted to determine if the officer is criminally culpable for his or her actions, as well as an administrative investigation to determine compliance with departmental policy.
2. These investigations, if both are required, may run simultaneously with the criminal investigation taking precedence.
3. To avoid improper contamination of the criminal investigation investigators will be well versed in the issues of *Garrity v. New York*. At no time will criminal investigators have access to any administrative investigative files. Criminal Investigators should provide access to their files to administrative investigators.
4. Upon arrival, investigators will first ensure the tasks itemized above have been completed. They shall then conduct their investigation, which will include the following:
  - a. The investigators will receive a general briefing and walk-through by the supervisory officer regarding the circumstances surrounding the shooting. The decision to conduct a walk-through with the involved officer present at this time must be made based on the following:
    - i. The type of investigation being conducted
    - ii. The physical and mental state of the officer
    - iii. The availability of the officer's attorney
    - iv. The circumstances at the scene
  - b. The investigators will make a thorough inspection of the scene and they will review the collection of all items and substances of evidentiary value, including photos and videotapes taken at the scene.

- c. The investigators will obtain recorded statements from the suspects.
  - d. The investigators will ensure that notification is provided to next-of-kin of injured or deceased suspects.
  - e. The investigators will locate and identify witnesses and conduct initial recorded interviews.
  - f. The investigators will record interviews with fire department personnel, emergency medical service providers, and other first responders to the scene.
  - g. They will conduct separate recorded interviews with each officer involved. (Involved officers will not be required to provide written or videotaped statements sooner than 48 hours after an incident.)
  - h. They will conduct the interview in a private location away from sight and hearing persons who do not have a need or a right to the information.
  - i. They will advise the officer not to discuss the incident with anyone except a personal or agency attorney, or departmental investigator until the conclusion of the preliminary investigation.
  - j. They will be cognizant of symptoms of post-traumatic stress, which might include time and space distortions, confusion, hearing and visual distortion, and emotional impairment, including shock. (Defer recorded interviews if these symptoms are evident.)
  - k. They will take any weapon fired by the officer into custody and handle it as evidence. Firearms shall be taken from officer in a discrete manner and the Officer in Charge shall ensure that arrangements are made to replace them with other firearms or advise the officer that they will be returned or replaced at a later time.
  - l. They will contact the medical examiner/coroner and obtain the autopsy report for any officer and/or suspect if required.
  - m. They will determine entrance and exit wounds, estimates of the shooter's position, the presence of alcohol or controlled substances, or other related evidence.
5. The results of any criminal investigation conducted will be presented to the Freestone County Attorney for grand jury review.

#### D. Post-Incident Procedures


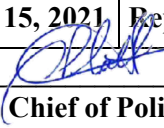
1. Involved personnel shall be removed from line duties pending evaluation but shall remain available for any necessary investigations.

2. All officers involved in the discharge of a firearm in the course of their duties will submit to an alcohol and drug screening at a location determined by the department, in accordance with city policy.
3. All officers directly involved in the shooting incident shall be required to contact an agency-designated specialist for counseling and evaluation as soon as practical after the incident. Involved support personnel should also be encouraged to contact such specialists after a shooting incident. After the counseling sessions, the specialist shall advise the agency as to the following:
  - a. Whether it would be in the officer's best interest to be placed on administrative leave or light duty, and for how long.
  - b. What will be the best course for continued counseling (The agency strongly encourages the families of the involved officers to take advantage of available counseling services).
  - c. If placed back on full duty and another deadly-force situation presented itself in the first work shift, would the officer be capable of defending himself/herself or another with the use of deadly force.
4. Any agency investigation of the incident shall be conducted as soon and as quickly as practical.
5. The agency should give a general briefing to other agency members concerning the incident so that rumors are kept to a minimum.
6. All personnel involved in a shooting incident should be advised that they are not permitted to speak with the media about the incident. Officers shall refer inquiries from the media to the Chief of Police, unless they are otherwise authorized to release a statement pertaining to the incident.
7. To protect against crank or abusive calls, officers should be advised to have phone calls answered by another person for several days if their names are released to the public.
8. Officers directly involved in the shooting incident shall be required to re-qualify as soon as practical.

#### E. Daily Stress Recognition

1. As post-traumatic stress disorders may not arise immediately, or the officers may attempt to hide the problem, each supervisor is responsible for monitoring the behavior of unit members for symptoms of the disorder.

2. If a supervisor believes that stress may be disrupting the officer's job performance or other life skills, the Chief of Police should be informed immediately. The Chief of Police may refer the officer back into counseling.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 6.4 CHAPLAINCY PROGRAM</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 _____ <b>Chief of Police</b>
	<b>Reference:</b>	

## I. CHAPLAINCY PROGRAM

The Chaplaincy Program of the Teague Police Department has been established to afford officers, employees, and their families the comfort of trained individuals to provide peer support and stress relief in post critical incident situations. A community-based volunteer support program system shall be in place to assist upon request. These volunteers will be qualified to ride with officers and provide a much-needed listening ear on a personal level, as well as a professional referral network.

## II. Purpose

The purpose of this policy is to establish a chaplaincy program to aid in officer mental health wellness.

## III. Peer Support Teams

- A. Designated volunteers who have completed chaplaincy training will form peer support teams for the purpose of being available for fellow officers, civilian employees, and family members when a critical incident occurs.
- B. Chaplaincy training will consist of a Department approved and recognized course of training provided and/or supervised by trained chaplains.

## IV. Community Based Volunteer Support System

- A. The Community Based Volunteer Support System will consist of persons from the community trained to assist employees and their families in critical incidents. These volunteers may ride with officers and provide support as deemed necessary by the Chief of Police.
- B. The goal of this System shall be:
  1. To provide a means of employee/employee's family with stress relief;

2. To provide a personal support system for employees and their families in times of need.

## **V. Professional Referral System**

- A. Designated Chaplains and Volunteers shall network with a group of professional mental health professionals to assist in Critical Incident Stress Debriefings. (see Policy 6.5 Support of Officer Involved in Critical Incidents)
- B. Introduction into the Professional Referral System of an employee will be at the discretion and with the approval of the Chief of Police.

## **VI. Confidentiality Requirements**

- A. All conversations between Chaplains and/or Mental Health Professionals and employees (or family members) will be held in the strictest of confidence.
- B. Confidentiality regarding such conversations will be governed by confidentiality laws as outlined in the State of Texas Counseling Codes.
- C. This confidentiality clause may only be breached if something illegal or life threatening to the employee or another is disclosed.
- D. A breach of this confidentiality clause may result in immediate expulsion of a Chaplain from this program.

## **VII. Mobilization of Chaplain(s)**

Chaplains may only be called to provide intervention by A Staff Officer (An Officer of the rank of Sergeant or above).


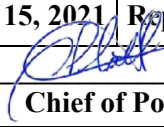
## **VIII. Limitations on Scope of Chaplain Support**

- A. Chaplains shall not attempt to offer legal advice to those receiving their services, under any circumstances;
- B. Chaplains should limit conversation to discussing the individual's feelings about an incident and to symptoms and experiences common to those who have been exposed to critical incidents.



## **IX. Voluntariness on the Part of Employee or Family Member**

- A. Officers and/or family members deemed in need of exposure to the Chaplaincy Program by those authorized to mobilize chaplains shall not be forced to receive such services.
- B. Officers and employees may be required to attend Critical Incident Stress Debriefings and/or other such services as outlined in Policy 6.5 or as designated by the Chief of Police.

	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 6.5 Support of Officers Involved in Critical Incidents</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>
	<b>Reference:</b>

## **I. SUPPORT OF OFFICERS INVOLVED IN CRITICAL INCIDENTS**

A “critical incident” is any event that has a stressful impact sufficient to overwhelm the usually effective coping skills of an individual. Critical incidents are abrupt, powerful events that fall outside the range of ordinary human experiences. These events can have a strong emotional impact, even on the most experienced officer. Every year, thousands of law enforcement officers are involved in intense critical incidents that can have serious long-term consequences for them and their family/friends. This policy describes a mechanism to provide support to officers involved in these types of incidents.

## **II. Assignment of a Support Partner**

The Chief of Police, or his designee, shall assign an officer to function as a support officer until the officer involved is escorted home. When possible, the support partner will be chosen by the officer involved. The support partner shall provide emotional support and needed assistance to the officer involved. The support partner shall not be involved in the investigation, nor act as a spokesperson for the officer involved. The support partner’s work schedule may be adjusted to accomplish this service.

## **III. Assignment of Hospital Guard**

The Chief of Police or his designee may assign a hospital guard if the officer requests a guard or there is reason to believe that reprisals might be planned against the injured officer. The work schedule of the officer performing guard duty may be adjusted to accomplish this service.

## **IV. Authorizing Transportation to Hospital for Family Members**

When an officer has been hospitalized for an injury while the officer is performing a peace officer function, the Chief of Police or his designee may assign another officer to transport the injured officer’s family members to the hospital.

## **V. On-scene Briefing of Involved Officers**

A. When an officer’s actions are being investigated following the death or serious injury of another person, the supervisor assigned to investigate the matter shall conduct a briefing with the officer involved. The briefing shall occur at the scene of the incident, if possible.

B. The officer's orientation shall include the following:

1. A brief description of the parallel investigation, covering Departmental policy and State law;
2. The reasons for an extremely thorough investigation;
3. The procedures of an Executive Staff Review;
4. The policy of placing the officer on administrative leave or duty; and
5. An estimate of the time it takes to complete an investigation.

#### **VI. Issuing a Replacement Weapon**

- A. When an officer turns over his weapon to an investigator following a shooting incident, the officer may be issued a replacement weapon.
- B. If possible, the replacement weapon should be issued at the scene of the incident.

#### **VII. Debriefing with Psychologist**

- A. When a critical incident has occurred, the Bureau Commander of the involved employee shall notify the Department contracted psychologist within 24 hours. The psychologist shall conduct a debriefing session for the officer in an expedient manner. The purposes of this debriefing are:
  1. To inform the employee of the normal symptoms and reactions associated with critical incidents and allow him to express his feelings; and
  2. To provide support and guidance to the officer in relation to dealing with the psychological after-effects of the incident.
- B. The debriefing is not related to any Departmental investigation of the incident and nothing discussed in the debriefing shall be reported to investigators.
- C. The critical incident stress debriefing shall be mandatory for all involved personnel and shall be conducted within 72 hours of the incident, or at the soonest practice time.

#### **VIII. Legal Debriefing**

Within 6 weeks of a critical incident in which an officer may be sued for civil liability, a City Attorney or other qualified attorney shall brief the officer. The briefing shall include an overview of the procedures in liability suits and a summary of the outcome of similar suits in Texas.

## **IX. Work Assignment While on Administrative Duty**


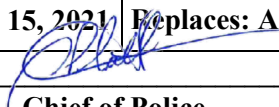
When an officer does not return to regular duty, pending an investigation of the critical incident, the Chief of Police may assign the officer to duties which serve the Department's needs and best uses the officer's skills and experience, if available.

## **X. Information about Executive Staff Review**

Following the Executive Staff Review of the investigation, an Executive Staff member shall meet with the officer to summarize their evaluation of the incident.

## **XI. Chaplaincy Program**

Designated officers or individuals who have completed chaplaincy training can provide peer support and stress relief for employees exposed to critical incident situations. (See Policy 6.4 Chaplaincy Program).

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 6.6 Mental Health Wellness Checkups</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
	<b>Reference:</b>	

## I. POLICY

Teague Police Department recognizes the necessity for routine mental health evaluations of officers employed with this agency. Officer mental health wellness is necessary for officers to maintain balance in both their professional and personal lives. It is, therefore, the policy of Teague Police Department that sworn employees will submit to annual mental health checkups by a departmental psychologist.

## II. PURPOSE

The Teague Police Department realizes there are mental stressors places on police officers due to occupational exposures, which may result from a specific incident or is cumulative over time. These occupational exposures may produce negative effects on the officer. Negative effects include depression, stress, burnout, Post Traumatic Stress Injuries (PTSI), Post Traumatic Stress Disorder (PTSD), and other related mental health conditions.

Having knowledge of negative effects to officers, because of occupational exposures to stressors, it is prudent for this department to afford officers the opportunity to discuss theses issues with a qualified mental health provider before the symptoms become insurmountable. Providing them the opportunity to meet with a psychologist, who is familiar with police culture, allows officers to discuss how they are doing and attain treatment plans for dealing with stress related symptoms.

Regrettably, many officers receive a psychological evaluation at the start of their career without the benefit of additional checkups over their career. This program requires each member of the department to visit with a departmentally designated psychologist once each year. The focus of this program is to let officers talk to a mental health specialist who understands what they do and the culture of law enforcement. Officer should be able to get help with any issues they may have and find ways to cope with the issues they are needing help.

## III. Mental Wellness Checkup Process

- A. Each sworn employee will have a specific date/time assigned to them for their appointment with the psychologist. Unless there are unusual circumstances, the appointment will be set during the week and during normal business hours. Emphasis on

minimal disruption of work scheduling will be taken into consideration for these appointments. Sworn employees may utilize departmental vehicles to travel to the appointment.

- B. Employees will be expected to make their appointment when it is scheduled. The employee shall notify their sergeant or the chief of police, in advance of their scheduled appointment, if they are unable to make the appointment for whatever reason. The appointment will be rescheduled.
- C. Employees will arrive at their appointment time, check in, and meet with the psychologist when scheduled. The psychologist may have tests that need to be completed before the interview portion of the appointment. Employees may discuss critical incidents that they have been involved in or impacted, work or personal issues causing stressors, or any other topics they feel are relevant during their appointment with the psychologist.


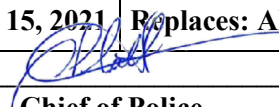
#### **IV. Mental Wellness Checkup Outcomes**

- A. There are different outcomes, after completion of the evaluation, based on the psychologist's assessment. They include:
  - 1. The employee has no apparently identifiable psychological issues. The psychologist notifies the department the employee made their appointment, and the employee returns to duty.
  - 2. The employee has some areas where the psychologist feels they may benefit from additional counseling. The psychologist may make some recommendations to the employee regarding follow-up for specific areas of concern. The employee has the option to go to additional sessions with a qualified mental health provider of their choosing. The psychologist notified the department the employee made their appointment, and the employee returns to duty.
    - a. The employee will need to schedule their appointments on their off days or coordinate with a supervisor to schedule leave time if they choose to attend counseling on their own after the mental health evaluation.
    - b. Workers Compensation may be contacted to determine if services would be covered under their guidelines.
  - 3. The psychologist identifies specific concerns with the employee. These concerns rise to the level that the psychologist does not believe, based on their professional opinion, the employee should return to work until the concerns are addressed. These concerns are normally a concern that the employee may pose a danger to themselves or others. In these cases, the psychologist will notify the department of their concerns. The employee will be placed on paid administrative leave for the first seven (7) days. The employee must do the following, to return to duty:

- a. Select a provider through the employer provided insurance and attend recommended services.
- b. Find a provider on their own and be responsible for any charges and addend recommend services.
- c. Schedule a follow up appointment with the departmental psychologist, once completing (a) or (b). The psychologist will evaluate the employee and determine if they are able to return to duty.
- d. The employee may return to their next scheduled shift, when cleared by the departmental psychologist within the first seven (7) days. However, the following steps will be taken if they are not cleared:
  - i. Accrued vacation, sick, and compensatory time can be used while going through this process.
  - ii. The employee may utilize the city sick leave pool, if qualified.
  - iii. The employee may explore short and/or long-term disability during this process.
  - iiii. Workers' compensation may be contacted to determine if the employee qualifies for this benefit.
  - iiiii. The employee will be required to continue with counseling until they are cleared for duty by the departmental psychologist.
- e. The employee may return to their next scheduled shift once the employee is cleared for duty by the departmental psychologist. The employee may be required to go through a short retraining course, if leave has been more than 28 days as determined on a case-by-case basis.
- f. Additional measures (possible personnel action) may be implemented if the employee is not cleared to return to duty within a reasonable time. The "reasonable time" may vary depending on the employee's circumstances. Any personnel action will be coordinated with the city administrator, city attorney, and workers' compensation representative if applicable.

## **V. Mental Wellness Checkup Follow Up**

- A. An email from the psychologist, stating the employee made their appointment, will be put in their medical file, once their appointment has been completed.
- B. There will be nothing negative associated with any employee who chooses to reach out for follow-up care on their own. This includes promotional opportunities and any other benefit normally afforded to all employees.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 6.7 Mental Health Leave</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b>	

## I. POLICY

Teague Police Department recognizes the necessity for routine mental health evaluations of officers employed with this agency. Officer mental health wellness is necessary for officers to maintain balance in both their professional and personal lives. It is, therefore, the policy of Teague Police Department that sworn employees involved in traumatic events be afforded appropriate leave to consult professional psychiatric services.

## II. PURPOSE

The Teague Police Department realizes there are mental stressors places on police officers due to occupational exposures, which may result from a specific incident or is cumulative over time. These occupational exposures may produce negative effects on the officer. Negative effects include depression, stress, burnout, Post Traumatic Stress Injuries (PTSI), Post Traumatic Stress Disorder (PTSD), and other related mental health conditions.

Having knowledge of negative effects to officers, because of occupational exposures to stressors, it is prudent for this department to afford officers the opportunity to discuss theses issues with a qualified mental health provider before the symptoms become insurmountable. Providing them the opportunity to meet with a psychologist, who is familiar with police culture, allows officers to discuss how they are doing and attain treatment plans for dealing with stress related symptoms.

Regrettably, many officers receive a psychological evaluation at the start of their career without the benefit of additional checkups over their career. This program requires each member of the department to visit with a departmentally designated psychologist once each year. The focus of this program is to let officers talk to a mental health specialist who understands what they do and the culture of law enforcement. Officer should be able to get help with any issues they may have and find ways to cope with the issues they are needing help.



### **III. DEFINITIONS**

- A. Traumatic event – an event which occurs in the peace officer(s) scope of employment when the officer is involved in the response to, or investigation of, an event that causes the officer to experience unusually strong emotional reactions or feelings which have the potential to interfere with their ability to function during or after the incident.

Traumatic events may include, but are not limited to, the following:

1. Major disasters which may include response to weather related events involving multiple casualties; or explosions with multiple casualties; or search and recovery missions involving multiple casualties;
  2. Incidents involving multiple casualties which may include shootings or traffic accidents;
  3. Line of duty death or suicide of a department member;
  4. Death of a child resulting from violence or neglect;
  5. Officer(s) involved shooting of a person.
- B. Mental health leave – administrative leave with pay granted in response to a traumatic event that occurred in the scope of the peace officer’s employment.
- C. Mental Health Professional – a licensed social or mental health worker, counselor, psychotherapist, psychologist, or psychiatrist.

### **IV. REQUESTING MENTAL HEALTH LEAVE**

An officer directly involved in a traumatic event may request the use of mental health leave. The request shall be made in writing through the chain of command. The request shall be treated as a priority matter and a decision on the granting of the leave shall be made no later than 24 hours following the submission of the request. The request shall be granted unless the chain of command can articulate specific compelling reasons to deny granting the leave.

A supervisor or coworker who becomes aware of behavioral changes in an officer directly involved in a traumatic event should suggest to the officer that he or she seek mental health leave and the assistance of a mental health professional. An officer’s failure to voluntarily seek mental health assistance shall be addressed by Policy 6.6.

### **V. CONFIDENTIALITY OF REQUEST**

Any request for mental health leave shall be treated as strictly confidential by all parties involved and shall not be discussed or disclosed outside the officer’s immediate chain of

command, and only as necessary to facilitate the use of the leave. Any officer or supervisor who becomes aware of behavioral changes and suggests the officer seek mental health leave shall not discuss that matter outside the chain of command. Any breach of this confidentiality shall be grounds for discipline.

Confidentiality may be waived by the officer seeking mental health leave. Confidentiality may be waived under circumstances which indicate the officer is a danger to himself or herself or others and department personnel must confer with mental health professionals.

## **VI. DURATION OF MENTAL HEALTH LEAVE**


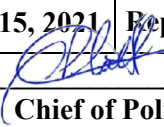
An officer directly involved in a traumatic event may request up to three working days of mental health leave.

Extensions of mental health leave may be available under certain circumstances. Any request for an extension shall be accompanied by documentation from a mental health professional who is counseling the officer. The request may extend the leave by three working days. Each officer may request no more than two extensions, each supported by sufficient documentation by the mental health professional. The Chief shall grant the extension(s) upon the receipt of sufficient documentation explaining the need for the extension.

## **VII. MENTAL HEALTH SERVICES AVAIABLE TO THE OFFICER**

Mental Health Services available to officers, dependent on their individual situations, can be attained through a variety of providers and other services. Such providers and other services can be, but not limited to, the following:

1. Personal Psychologist/Psychiatrist through city provided health insurance company.
2. Departmental Contracted Psychologist – SafeGuard Psychological Services 2301 Bagdad Road, Suite 104, Cedar Park, Texas.
3. The services of Dr. Tania Glenn and Associates, PA 1001 Cypress Creek Road Suites 403, Cedar Park, Texas.
4. Law Enforcement Management Institute of Texas (LEMIT) Post Critical Incident Seminar specifically designed for the first responders who have been adversely affected by highly traumatic events.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.0 Constitutional Safeguards</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: TEXAS BEST PRACTICES: 7.04</b>	

## I. POLICY

The federal and state constitutions guarantee every person certain safeguards from unreasonable government intrusion into their lives. These safeguards have become the cornerstone for the application of criminal justice in America. The department expects officers to observe constitutional safeguards. The department further expects that officers understand the limits and prerogatives of their authority to act. Respect for the civil liberties of all persons shall be the paramount concern in all enforcement matters.

## II. PURPOSE

The purpose of this policy is to define the legally mandated authority for the enforcement of laws; to establish procedures for ensuring compliance with constitutional requirements during criminal investigations; to set forth guidelines concerning the use of discretion by officers; and to define the authority, guidelines, and the circumstances under which officers should exercise alternatives to arrests and pretrial confinement.

## III. THREE LEVELS OF ENCOUNTERS

There are only three levels of encounters between civilians and police officers: consensual encounters, temporary detentions, and arrests. Detentions and arrests are considered seizures of the person for purposes of constitutional analysis.

To be lawful a consensual the encounter must be voluntary as seen through the eyes of a reasonable person. In other words, if a reasonable person would not believe he or she could simply walk away from the encounter, then the encounter shall be considered a seizure by the courts.

To be lawful a temporary detention must be based upon reasonable suspicion, i.e. specific, articulable facts and circumstances that would lead a reasonable officer to conclude criminal activity is afoot.

To be lawful and arrest must be based upon probable cause, i.e. specific articulable facts and circumstances that would lead a reasonable officer to conclude a specific person had committed a specific crime.

Reasonable suspicion and probable cause are evaluated by analyzing the totality of the information known to the officer at the time a person is seized. Information discovered incident to a detention, or an arrest, cannot retroactively support the seizure.

#### **IV. PROBABLE CAUSE AND REASONABLE SUSPICION**

A. Probable Cause: in all circumstances an officer must have probable cause to make an arrest. Probable cause is also required in most circumstances to search, but there are some exceptions to that requirement.

1. According to the U.S. Supreme Court, "Probable cause exists where the facts and circumstances within their [the arresting officers'] knowledge and of which they had reasonable trustworthy information are sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed." See 7.3 for additional information.
2. When an officer has sufficient probable cause, he or she may arrest or, in certain circumstances, search a person. The purpose of an arrest is to make a formal charge. While formal charges may not be filed for any number of reasons, officers should make a custodial arrest only if a formal charge is anticipated.
3. The test for evaluating the existence of probable cause is based on the totality of the circumstances known to the officer at the time of the arrest.

B. Reasonable Suspicion:

An officer must have reasonable suspicion to temporarily detain a person. The purpose of a detention is to further the investigation into potential criminal activity

1. Reasonable suspicion involves a somewhat lower standard than probable cause, generally defined by the courts as a circumstance or collection of circumstances that would lead a trained, experienced officer to believe that criminal activity may be afoot. The same types of facts and circumstances which can be used to build probable cause can also be used to build reasonable suspicion. The test for evaluating the existence of reasonable suspicion is the same test used to evaluate probable cause: the totality of the circumstances known to the officer at the time of the detention.
2. When an officer has reasonable suspicion, he or she may detain a person for a temporary period of time during which time the officer must work efficiently towards confirming the need for the continued detention of the person, or the release of the person detained. Officers have greater authority to detain a suspect in a crime as opposed to a witness to an offense. "Temporary period of time" shall mean only that relatively brief amount of time that an officer may detain a person, so the officer may initiate or continue the investigation, having reasonable suspicion to believe the person is involved in the criminal activity. Once the officer has determined that he or she has insufficient facts and circumstances to establish probable cause or is not likely to obtain sufficient facts or circumstances to establish probable cause, the officer shall release the person.

3. Frisk authority: officers do not have the authority to automatically frisk a person who has been detained. The frisk has one lawful purpose – to ensure the safety of the officer. In order to support a claim that the officer was at risk the frisking officer must articulate what the detainee was doing at that moment in time that caused the officer to be concerned for his or her safety.

## V. AUTHORITY AND DISCRETION

### A. Law-enforcement authority:

State law invests peace officers with authority to prevent crime, apprehend criminals, safeguard life and property, and preserve the peace. These goals are accomplished by enforcing state and local laws and ordinances. Texas restricts a peace officer authority with regards to making warrantless arrests. In order to perform a warrantless arrest under Texas law an officer must have probable cause to believe the person to be arrested committed the offense and there must be a specific statute which authorizes the warrantless arrest in that situation. Warrantless arrest authority is found primarily in Chapter 14 of the Texas Code of Criminal Procedure but is also found in other statutes. It is the officer's responsibility to confirm that such statutory authority exists.

### B. The use of discretion by officers

1. While officers have the authority to arrest an offender under many circumstances, they seldom can make an arrest for every offense they observe. Officers must prioritize their activities to provide the highest level of service to their community. As a result, they must often use discretion in deciding the level of enforcement action based on the circumstances.
2. Departmental policy gives officers procedures to follow for common or critical enforcement tasks. Departmental policies and procedure are to be followed unless unusual or extreme circumstances dictate another course of action. In these cases, officers shall make reasoned decisions in their discretion based on good judgment, experience, and training. It is up to the individual officer to consider the relevant facts, the situation, and then, using knowledge, training, and good judgment, make appropriate decisions. Supervisors must closely observe the use of discretion by their subordinates and point out factual errors or alternatives that may be more appropriate.
3. Officers should understand that their decisions regarding arrests and searches are in all cases subject to review by their supervisors. Additionally, these decisions are subject to review by prosecuting attorneys, defense attorneys, and judges.
4. Supervisors shall observe and review the activities of officers and counsel them as needed regarding the use of discretion. In addition to counseling, officer's decisions are subject to review and discipline through the chain of command.

### C. Alternatives to arrest/pre-arraignment confinement

1. Officers are required to arrest suspects for all felony offenses and those major misdemeanor offenses where a victim was injured, property was stolen or damaged, or the public or an individual was placed at risk of great harm. Officers shall only make warrantless arrests in situations authorized by state law. In all other situations an officer shall obtain an arrest warrant.

If the immediate arrest of a suspect is not advisable due to the suspect's health, age, infirmity, or family situation, the officer should contact a supervisor for disposition. A supervisor or the Chief of Police can authorize the officer to release the individual and seek a warrant for an arrest at large. Once the arrest is made and the suspect is transported to jail, the officer may contact the magistrate to see if the individual can be released on his own recognizance.


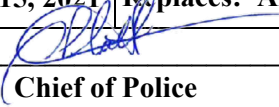
2. In misdemeanor criminal cases where there is no victim or property loss, where an individual or the public was not placed in danger of great harm, and in traffic offenses, officers may occasionally be faced with situations where formal action is not advisable. In such cases, officers may elect to exercise alternatives, such as the issuance of citations, referral to a social service agency, or simply to give a warning.
3. In determining whether a citation should be used, the officer shall:
  - a. Decide whether the offense committed is serious.
  - b. Attempt to understand the contributing factors to the incident and evaluate whether a reasonable person would be influenced by those factors.
  - c. Make a judgment as to whether the accused poses a danger to the public or himself/herself.
4. Officers often deal with situations where the public interest would be better served by social service agencies, crisis, and/or professional organizations. In such cases the officer may refer the person to an appropriate social services agency if the person is agreeable to such a referral.
5. The use of warnings may sometimes provide a solution to a problem and may enhance the public perception of the department. Normally, the use of a warning occurs in traffic offenses, but occasionally may be applied to other criminal offenses. In determining if a warning should be issued, the officer shall consider:
  - a. The seriousness of the offense.
  - b. Whether a victim was injured or had property damaged by the offender.
  - c. Attempt to understand the contributing factors to the incident and evaluate whether a reasonable person would be influenced by those factors.
  - d. The likelihood that the violator will heed the warning.

### III. PROTECTION OF INDIVIDUAL RIGHTS

- A. Officers will always act to preserve and protect the rights of all persons.
- B. Miranda warnings are required prior to any custodial interrogation. A custodial interrogation occurs when a person is not free to leave and is asked questions that are intended to elicit an incriminating response. Officers are expected to understand the requirements of the Code of Criminal Procedure, articles 38.22 and 2.32 before taking any statements from suspects. All custodial interrogations shall be video or audio recorded. If the custodial interrogations are not recorded, the officer conducting the interrogation shall explain why in the officer's report.
  1. Listed below are representative examples of situations that may not require a Miranda warning.
    - a. Questioning during a routine traffic stop or for a minor violation, which includes driving while intoxicated (DWI) stops until a custodial interrogation begins. Such questions may include, but are not limited to, inquiries about vehicle ownership, the driver's destination, the purpose of the trip, and insurance documents. Any questions focusing on the person's participation in criminal activity may require warnings.
    - b. During routine questioning at the scene of an incident or crime when the questions are not intended to elicit incriminating responses.
    - c. During voluntary appearances at the police facility when a suspect is not in custody but is responding to questions designed to elicit incriminating responses.
    - d. When information or statements are made spontaneously, voluntarily and without prompting by police. (Note: Follow-up questions that exceed simple requests for clarification of initial statements may require Miranda warnings.)
  2. Administering Miranda.
    - a. Miranda warnings shall be read by officers from the card containing this information to all persons subjected to custodial interrogation. Officers shall confirm that the warning text on the card matches the warning language found in article 38.22 of the Code of Criminal Procedure.
    - b. Freelancing, recitation from memory or paraphrasing the warnings is prohibited because it precludes officers from testifying in court as to the precise wording used.
    - c. Officers shall ensure that suspects understand their right to remain silent and their right to an attorney. Suspects may be questioned only when they have knowingly and intelligently acknowledged they understand their rights and have affirmatively waived those rights. Threats, false promises, or coercion to induce suspect statements are prohibited.

- d. Waivers of the Miranda rights must be performed affirmatively and shall be audio or video recorded as required by state law. If a recorded statement is not an option, the statement shall be in writing as required by state law.
- e. Officers arresting deaf suspects or those suspects that appear to have limited proficiency in English shall notify their immediate supervisor and make arrangements to procure the assistance of an interpreter in accordance with this agency's policy or state and federal law.
- f. The administration of the Miranda warning shall be recorded. State law prescribes those circumstances under which a non-recorded statement might be admissible. Officers shall comply with state law in these matters.



	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 7.1 Field Interview, Consensual Encounters and Detentions</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____ <div style="text-align: center;">   <b>Chief of Police</b> </div>
	<b>Reference: TEXAS BEST PRACTICES: 7.07</b>

## I. POLICY

Per the US Supreme Court, there are only three types of encounters between police and civilians: (1) a consensual encounter in which the civilians voluntarily elect to stay and interact with the officer, (2) a detention based upon reasonable suspicion, which may include a frisk for weapons if the officer can state the facts and circumstances that justify the officer's fear for their safety, and, (3) an arrest based upon probable cause. This agency expects and encourages officers to conduct field interviews. Field interviews are important contacts with individuals that aid in preventing and investigating crime. This agency expects officers to gather information with proper observance of constitutional safeguards. Strict constitutional guidelines exist that protect both the civil rights of all persons and the need of officers to obtain information crucial to the reduction and prevention of crime.

## II. PURPOSE

The purpose of this policy is to clearly establish the difference between a consensual encounter and an investigative detention or stop, and to assist officers in determining what compliance is required during field interviews and when frisks for weapons are lawful, necessary, and useful, and to establish procedures for conducting both safely. (TEXAS BEST PRACTICES: 7.07)

## III. DEFINITIONS

- A. Field interview: A brief interview of a person to determine the person's identity and to gather information or to resolve the officer's suspicions about possible criminal activity or to determine if the person has information about a criminal offense. A field interview may take place during a consensual encounter or during a temporary detention. The difference is in the information known to the officer at the outset of the encounter which establishes the encounter as either consensual in nature or a temporary detention based upon reasonable suspicion. Field interviews require voluntary cooperation of the subject for purposes of answering questions.
- B. Frisk: A "pat-down" search of outer garments for weapons.
- C. Reasonable suspicion: Articulable facts that, within the totality of the circumstances, lead an officer to reasonably suspect that criminal activity has been, is being, or is about to be committed. The reasonableness of an officer's actions will be determined by reviewing the totality of circumstances known to the officer at the time he or she takes the action.

- D. Detention also known as an investigative detention, stop, Terry stop, Terry Frisk, or stop-and-frisk: Requiring an individual to remain with the officer for a brief period for the purpose of investigating the actions of the individual. To make the stop, the officer must have reasonable suspicion to believe that criminal activity is afoot and that the person to be detained or stopped is involved. The combination of facts and circumstances must lead a reasonable officer to believe that the person to be detained is involved in criminal activity. It is not permissible to detain a person based upon mere suspicion or the officer's inarticulate hunch that the person is up to no good.

The following list of factors and circumstances may be used to build reasonable suspicion. This list is not all-inclusive nor is the presence of any one of these circumstances alone enough for reasonable suspicion.

1. Officer has knowledge that the person has a criminal record.
2. A person fits the description of a wanted person.
3. A person has exhibited furtive conduct, such as attempting to conceal an object from the officer's view.
4. The appearance, behavior, or actions of the suspect indicate the person is involved in criminal activity.
5. The time of day or night.
6. The officer observes a vehicle that matches that of a broadcast description of a suspect vehicle.
7. A person exhibits unusual behavior, such as staggering or conduct indicating a need for medical assistance.
8. The suspect is in geographical and temporal proximity to the crime scene.
9. The suspect is carrying an unusual object, or his/her clothing bulges in a manner consistent with concealing a weapon.
10. Flight from the officer may be considered as a fact or circumstance, but mere flight alone, without additional facts or circumstances, will be insufficient to establish reasonable suspicion.
11. Firsthand observations by the officer.
12. Information from informants or members of the community.
13. Collective knowledge or information shared by other officers.
14. Reasonable inferences made by the officer from information known to the officer.

E. Consensual encounter:

Is an encounter between a police officer and a civilian in which a reasonable person would believe, based upon the circumstances of the encounter, that compliance is not mandatory and he or she is free to decline to talk with the officer and is free to leave.

#### IV. CONSENSUAL ENCOUNTERS

A. Making the consensual encounter

1. An officer may conduct a field interview at any time if an individual is willing to speak with the officer. A field interview requires voluntary cooperation from the individual. The individual may decline to answer any, or all, questions during either a stop or consensual encounter. The individual may leave at any time during a consensual encounter. The individual may refuse to produce identification or otherwise identify himself/herself during either a consensual encounter.
2. The officer shall articulate all the reasons for contacting the individual in the first place. The officer shall explain all the steps taken in contacting the individual. Officers should note that if the initial encounter is deemed a seizure by the court, the officer will be required to justify his/her initial detention by describing specific and articulable facts which, taken together with rational inferences from those facts, established reasonable suspicion for that detention. See III. D. above.

B. Place of the interview

1. Generally, field interviews may be conducted anywhere the officer has a right to be, including the following:
  - a. City-owned or controlled property, normally open to members of the public.
  - b. Areas intended for public use or normally exposed to public view.
  - c. Places to which an officer has been admitted with the consent of the person empowered to give such consent.
  - d. Places where circumstances require a lawful immediate law enforcement presence to protect life, well-being, or property.
  - e. Areas where an officer may be admitted pursuant to a lawful arrest or search warrant.
2. Consensual encounters or stops shall not be done to coerce a person to leave an area or place where he or she has a legitimate right to be and where no violation of law has occurred.

C. Conduct of Interviews during a Consensual Encounter

1. Officers shall clearly identify themselves and, if not in uniform, display identification.

2. As noted above, a person participating in a consensual encounter with an officer may discontinue the interview at any time. To repeat, during a consensual encounter, persons shall not be detained in any manner against their will nor shall they be required to answer questions or respond in any manner if they choose not to do so. Since the distinction between a consensual encounter and a detention depends to a great extent on whether, under the circumstances, the subject perceives that he/she is free to leave, officers shall comply with the following guidelines:
  - a. All requests during the interview should be phrased with neutral or optional words, such as "may," "would you mind," etc.
  - b. The duration of an interview should be as brief as possible unless it is prolonged by the subject.
  - c. During the interview, officers should confine their questions to those concerning the suspect's identity, place of residence, and other matters necessary to resolve the officer's suspicions.
  - d. Miranda warnings are not required during consensual encounters. The warnings are not required until custodial questioning takes place.
3. The success or failure in obtaining information beneficial to crime analysis and criminal investigation will depend upon an officer's ability to put individuals at ease and establish rapport. However, during a field interview, if the person should ask whether he/she must respond or indicate that he/she feels compelled to respond, the officer shall immediately inform him/her of the right to refuse and the right to leave.
  - a. When a person refuses or ceases to cooperate during an interview, the refusal itself cannot be used as the basis for escalating the encounter into a detention.
  - b. Individuals cannot be compelled to answer any questions during field interviews conducted during consensual encounters.

## **V. INVESTIGATIVE DETENTION OR STOP (and frisk when warranted)**

- A. The legal authority to conduct an investigative detention or stop (and frisk when warranted) is based in federal and state constitutions as interpreted by court decisions. A frisk is defined as a limited search for weapons.
- B. Investigative detentions may involve two distinct acts. The first is the actual detention or stop and it is based on reasonable suspicion. A second component may be a frisk of the detainee for weapons. The frisk must be justified by the officer's reasonable fear for his/her safety during the detention. The safety concern must arise from the conduct of the detained person, not from safety concerns in general. For example, a frisk could not be justified solely on the claim that "all drug dealers are dangerous." Not every detention will result in a frisk. Examples of safety factors justifying a frisk may include but are not limited to the following:

1. The type of crime being investigated, particularly those involving weapons.
2. When the officer must confront multiple suspects.
3. The time of day and location of the stop.
4. Prior knowledge of the suspect's propensity for violence.
5. Any indication that the suspect is armed.
6. Age and sex of the suspect. Officers shall exercise caution with very young or very old people or persons of the opposite sex.
7. Demeanor of the suspect.
8. Failure or refusal to follow simple commands.
9. Statements made by the suspect.
10. Aggressive actions or statement made by the suspect.

C. Manner of conducting a frisk

1. Ideally, when staffing permits, two or more officers should conduct the frisk, one to search and the other to provide protective cover.
2. The minimally intrusive nature of a frisk permits the suspect to be searched while standing, or with hands placed against a stationary object, feet spread apart, which is the preferred method.
3. When frisking, officers shall pat-down only the external clothing for objects that reasonably could be weapons and remove them. Retrieval of the weapon may give probable cause to arrest. If so, officers may then conduct a complete custodial search of the suspect incident to arrest.
4. If, during a lawful detention based on reasonable suspicion, the officer conducts a frisk and feels an object whose contour or mass makes its identity as contraband immediately apparent, pursuant to the plain-touch doctrine, it may be withdrawn and examined.
5. If the suspect is carrying a bag, purse, suitcase, briefcase, sack, or other container that may conceal a weapon, officers may squeeze the container to determine if it contains a weapon. Officers shall not open the container, without consent, but shall place it beyond the subject's reach for the duration of the stop.

#### D. Protective search

Under some conditions, the protective frisk may be extended beyond the person detained. This frisk occurs most often with vehicles. A lawful, protective search for weapons, which extends to an area beyond the person in the absence of probable cause to arrest, must have all the following elements present:

1. A lawful detention as defined herein, or a lawful vehicle stop.
2. A reasonable belief that the suspect poses a danger.
3. A frisk of the subject must occur first.
4. The search must be limited to those areas in which a weapon may be placed or hidden.
5. The search must be limited to an area that would ensure that there are no weapons within the subject's immediate grasp.
6. If the suspect has been arrested and removed from immediate access to the vehicle, a search of the vehicle cannot be made for protective reasons. The protective frisk of the vehicle may only occur if the suspect is to be returned to the vehicle. A search may be made of the vehicle if other exceptions to a search warrant exist.

#### E. Period of detention:



Investigative detention must be conducted as quickly as possible. Once the detaining officer determines that the basis for reasonable suspicion no longer exists, or that additional facts and circumstances are not being developed, the person detained shall be released. Should the initial reasonable suspicion be reinforced with additional information that develops probable cause, the period of detention could be lengthened. The courts have not established an exact time limit for detentions, but case law suggests detentions are measured in increments of less than an hour.

### **VI. DOCUMENTING THE INTERVIEW OR STOP**

For purposes of successful prosecution and of defending departmental actions to the public, all field interviews and investigative detentions must be recorded. The following methods will be utilized:

- A. Patrol officers will record all field interviews in their entirety on the in-car audio video systems. Officers will attempt to position the vehicle or camera in a position to record the interview. If not possible, the use of the audio portion is required.
- B. If an interview or investigative detention results in an arrest, the arresting officer will clearly detail the reasonable suspicion that led to the interview or detention in the narrative of the arrest report as well as maintaining the audio/video recording as evidence.

- C. Officers not equipped with in-car or portable audio/video recording systems will obtain a service number and create an incident report entitled “Field Interview” and record the reasonable suspicion and details of the interview of detention. The report will be forwarded through the officer’s supervisor to the records unit.

	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 7.2 Arrests with and Without A Warrant</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____ <div style="text-align: center;">   <b>Chief of Police</b> </div>
	<b>Reference: TEXAS BEST PRACTICES: 7.02, 7.03, and 7.04</b>

## I. POLICY

Short of the application of force, an arrest is the most serious action an officer can undertake. Being arrested can cause repercussions throughout a person's life, even if eventually found not guilty or never brought to trial. It is of paramount importance that officers not undertake an arrest without the utmost care.

There are two important legal questions facing officers making an arrest in Texas. The first deals with the existence of probable cause. Without probable cause, the arrest violates the Fourth Amendment and any evidence that flows from the arrest is inadmissible. Secondly, the State of Texas mandates that any warrantless arrest by an officer must be authorized by statute. (See generally Ch. 14, Code of Criminal Procedure.) Officers shall accordingly exercise critical judgment in making arrests. Critical judgment includes consideration for bystanders, the time, place, and location of offenses, the presence of probable cause and statutory authority and the use of force that may be required to make the arrest.

Officers shall consider alternatives to arrest consistent with their law-enforcement mission.

## II. PURPOSE

The purpose of this policy is to define the authority of officers to make arrests and to outline the mechanism for making an arrest with and without a warrant.

## III. DEFINITIONS

- A. Arrest: An arrest is the physical seizure of a person, and it must be supported by probable cause.



- B. Probable cause: According to the U.S. Supreme Court, "Probable cause exists where the facts and circumstances within [the arresting officers'] knowledge and of which they had reasonable trustworthy information are sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed and that the person to be arrested committed it." An officer must have probable cause to obtain a warrant or to make a warrantless arrest. Generally, probable cause has been interpreted to mean – specific and articulable facts and circumstances known to the officer that would cause a reasonable officer to conclude that a specific person has committed a specific offense.

#### **IV. DISCRETION**

- A. Officers shall demonstrate discretionary judgment. Discretion shall be applied reasonably and shall be guided by the oath of office, the limits of authority as established by law, the decisions and interpretations of the courts, the policies of this department, and any instruction provided by supervisors.
- B. Officers shall not make arrests or take any enforcement action based in whole or in part on a person's sex, race, creed, color, age, general or assumed attitude, ethnic or natural origin, economic status, disabilities, or sexual orientation. The exception to this policy is that race and/or other identifying characteristics listed above may be used to build probable cause if they are relevant factors identifying a suspect.

#### **V. ARRESTS WITH A WARRANT (TEXAS BEST PRACTICES: 7.02)**

- A. General Procedures for Obtaining an Arrest Warrant and Arresting with a Warrant.
1. Obtaining an arrest warrant will be made pursuant to Chapter 15 of the Texas Code of Criminal Procedure (TCCP). All officers shall become familiar with the specific language/laws concerning obtaining arrest warrants found in Chapter 15 of the TCCP. The following are shortened versions of Articles 15.01, 02, 03, and 05. If departmental approval is received, an officer may obtain an arrest warrant by following these requisites:
    - a.(15.01) An arrest warrant is a written order from a magistrate, directed to a peace officer commanding the officer to arrest a person accused of an offense that is to be dealt with according to law.
    - b. (15.02) A warrant must be issued by a magistrate, in the name of the State of Texas, and must specify the name of the person to be arrested or a reasonable, definite description of the person. The warrant must state that the person is accused of a crime and name the crime. The warrant must be signed by a magistrate and it must indicate the identity of the magistrate's office.
    - c.(15.03) A magistrate in the State of Texas may issue an arrest warrant when a person (the officer) makes an oath (affidavit or complaint) that another has committed an offense against the laws of the State of Texas.

- d. (15.05) An officer's complaint or affidavit must state the name of the accused or some reasonably definite description of the individual. It must show directly that the person has committed a crime or that there is good reason to believe that the person has committed a crime. The complaint/affidavit must state the time and place of the offense, as definitely as can be done by the affiant, and it must be signed by the affiant.
2. Unless assigned as an investigator or detective, officers will obtain supervisory approval before applying for an arrest warrant for any individual.
3. All members of the department will utilize approved affidavit and arrest warrant forms provided by the department. Upon completion of the affidavit and warrant, all officers shall have the documents reviewed and approved by a supervisor prior to requesting judicial approval.
4. Warrants will be carried only to the judge of the municipal court or to a county or district court judge for judicial review. If a warrant approval is refused by any judge, the affidavit and warrant shall not be taken to any other judge until substantial additional information proving probable cause has been added to the affidavit. Subsequent reviews will be done by the same magistrate unless he/she is unavailable. If the same magistrate is unavailable, the officer shall inform the new magistrate that the original affidavit was refused and provide the reason(s) why it was refused.
5. Except as authorized by the Texas Code of Criminal Procedure, Chapter 14, or Section 18.16, an officer shall not arrest anyone without an arrest warrant.
6. An officer shall not alter any information on an arrest warrant in any manner after a magistrate has issued it.
7. An officer shall presume that any arrest warrant which appears in proper form is valid. To be in proper form and valid on its face, an arrest warrant shall have the following features:
  - a. Be issued in the name of "The State of Texas"
  - b. Specify the name of the person whose arrest is ordered, or provide a reasonable description if the name is not known
  - c. State that the person is accused of a named offense
  - d. Be signed by a magistrate whose office must be named.
  - e. Contain the court seal on the warrant.
8. An officer shall execute a valid arrest warrant as provided by law and departmental policies.

9. If the arrest warrant lacks proper form, the officer shall not execute the warrant, but shall return the warrant to the magistrate who issued it.
10. An officer who has any question about the details or validity of an arrest warrant shall attempt to verify the information before making an arrest under authority of that warrant.
11. Whenever practical, an officer shall automatically verify the currency of any arrest warrant issued thirty days or more before the date of execution.
12. Any decision to send regional or statewide messages concerning a warrant will be made by a supervisor or the investigator assigned to the case.
13. An officer need not have actual physical possession of an arrest warrant to execute it. However, before executing a warrant not in his possession, the officer shall personally determine the location of the warrant and shall ensure that the arrestee sees a copy of the warrant as soon as possible after his/her arrest.
14. In executing an arrest warrant, regardless if the warrant in possession or not, an officer shall announce to the person being arrested that the arrest is made pursuant to an arrest warrant. An officer has the warrant in his possession shall show it to the arrestee. If the officer does not possess the warrant, he/she shall advise the arrestee of the charge, the bond, and the originating agency that issued the warrant.
15. Officers may enter a third party's residence in any of the following situations:
  - a. With consent to search from the resident or person having control of the property,
  - b. With a search warrant for that residence to enter and make the arrest, or
  - c. While in fresh pursuit of the wanted person in felony cases only.

#### B. Warrants from Other Jurisdictions

1. If an officer has knowledge that another Texas law-enforcement agency holds a valid arrest warrant for a person, the officer may arrest that person. If an officer makes an arrest on a warrant from another Texas law-enforcement agency, the officer shall do the following:
  - a. Arrest the defendant.
  - b. Notify the agency holding the warrant that this department executed the warrant and give the location of the arrestee.
  - c. An officer shall also execute an arrest warrant telegraphed under the authority of a Texas magistrate, or through teletype messages through the Texas Law Enforcement System (TLETS) once confirmation has been made.

2. The department shall hold the arrestee as the magistrate prescribes until releasing the arrestee to the custody of the department holding the warrant, if the department holding the warrant can reasonably take custody of the person in a timely manner. Otherwise, until transferring the person to the custody of the county sheriff's department.

#### C. Warrants from Other States:

When any officer has probable cause to believe that a person stands charged of a felony in another state, the officer shall do the following:

1. Arrest the person only after the warrant has been confirmed using accepted methods of warrant confirmation. (Such an arrest is made under the authority granted to Peace Officers in the Texas Code of Criminal Procedure, Chapter 51, Fugitives from Justice)
2. Book the arrested person directly into the custody of the county sheriff's department.
3. The existence of a warrant from another state does not provide officers the authority to enter a third person's residence to make the arrest. Officers may only enter a third person's residence in the following circumstances:
  - a. With consent to search from the resident or person having control of the property
  - b. With a search warrant for that residence to enter and make the arrest, or
  - c. While in fresh pursuit of the wanted person.

#### D. Chance Encounters

1. An officer who lawfully stops or otherwise detains and identifies a person may concurrently initiate a records check to determine whether any arrest warrant is outstanding against that person.
2. An officer may detain a person whom he/she has lawfully stopped for a reasonable time to conduct a routine records check by radio, telephone, teletype, or computer terminal. However, detention may be extended, but no longer than necessary, if the officer has a reasonable suspicion that a warrant is outstanding.
3. The detained person may be required to wait in the officer's vehicle, in his/her own vehicle, or in some other convenient place.
4. The person may be frisked if the officer can articulate a reasonable fear for his/her safety.

#### E. Planned Executions of Arrest Warrants

1. Prior to executing an arrest warrant, the officer in charge shall notify his/her chain of command.
2. The time of day for executing the arrest warrant shall be based on the following rules:
  - a. Execute during daylight unless circumstances make this dangerous or impractical.
  - b. Execute when the person named in the warrant is most likely to be present.
  - c. Execute when resistance is least expected and best controlled.
  - d. Execute to minimize the danger or inconvenience to other persons who may be on the premises unless other circumstances make this impractical.
  - e. Whenever possible, arrests shall be made in a location where the arrest will not pose a threat to the safety of the public, as it might in, e.g., crowded places where bystanders may be injured should the arrestee offer resistance, particularly resistance involving the use of firearms.
3. An officer may serve the warrant at any place, public or private, where the individual named is reasonably believed to be located (subject to the third-party, private-location rule.)
4. Officers need not execute the warrant at the first possible opportunity but may choose the time and place in accordance with these rules.
5. An officer shall not select the time and place of arrest solely to embarrass, oppress, or inconvenience the arrestee.
6. An officer shall not use force to enter private premises to execute a misdemeanor arrest warrant, without having a search warrant.
7. In general, when seeking to enter a private premise, an officer shall ring the doorbell or knock on the door, announce his/her intentions and purpose, and demand admittance. He/she may then wait for a reasonable time under the circumstances to be admitted.
8. Officers may only enter a third person's residence in the following circumstances:
  - a. With consent to search from the resident or person having control of the property,  
or
  - b. With a search warrant for that residence to enter and make the arrest, or
  - c. While in fresh pursuit of the wanted person in cases of felony.
9. If the execution of an arrest warrant may involve significant risk to officers, a statement of the circumstances of this risk should be included in the affidavit with a

request that the magistrate include a “No Knock” authorization to the warrant. If a “No Knock” provision has not been authorized by the magistrate, and articulable circumstances occur at the time of execution of the warrant (such as efforts to destroy evidence, evade arrest, or endanger officers) an immediate entry may be made without the required notice and waiting period.

10. An officer who must make a forcible entry shall enter the premises by the least forceful means possible under the circumstances. Although entry may necessarily include breaking a door or window, an officer must strive to inflict as little damage as possible to the premises.
11. When it is necessary to forcibly enter private premises to execute a felony arrest warrant, the officer in charge of the operation shall have enough officers present, and take other appropriate measures, to protect the safety and security of all persons present. To identify the group as officers, at least one fully uniformed officer should lead the entry into the premises.
12. After forcibly entering private premises to execute a felony arrest warrant, officers shall immediately secure the premises by locating and controlling the movement of all persons who reasonably appear to present a threat to the safety of the officers. Officers shall also control any object that may be used as a weapon. An officer may frisk any person whom the officer reasonably suspects may have a weapon concealed upon his/her person.
13. Officer shall leave the premises at least as secure as when they entered by leaving it in the hands of a responsible person or by locking all doors and windows. If the premises are left unsecured, a guard will remain until the site can be turned over to a responsible party or otherwise secured from illegal entry.

#### F. Execution of Locally Issued Warrants by Other Jurisdictions

1. When another law-enforcement agency within Texas holds a prisoner on a warrant from this department, this department will make necessary arrangements to have the person picked up.
2. When an out-of-state department notifies this department that the out-of-state department has executed a felony arrest warrant held by this department and is holding the person arrested, this department shall immediately pursue extradition proceedings.

#### G. No-Book Warrant Procedures

1. For Class C warrants issued by this city, an officer may allow a violator to pay fines in full, during normal business hours, rather than booking the violator into the holding facility.
2. Officers who wish to serve Class C municipal warrants without booking the defendant into the holding facility should follow these procedures:

- a. Confirm that the warrant matches the identity of the person detained.
- b. Confirm that the defendant has enough cash to pay the full amount of the fine(s) or he/she can obtain the cash quickly.
- c. If the defendant has the cash necessary or can obtain the cash quickly, the officer should ascertain if the defendant has transportation. The officer should follow the defendant to the police department for disposition of the fines.
- d. Upon arrival at police department the officer should obtain the original warrant and complete the officer's return on the warrant, after payment in full has been made.
- e. The officer should complete a warrant arrest report.
- f. The violator will pay the complete amount of all fines to the clerk. **Officers are prohibited from handling any of the cash during any part of this transaction.**
- g. The officer should ensure that the defendant is provided a receipt for the payment.
- h. If after a reasonable time has elapsed as determined by the officer or the officer's supervisor, the defendant is unable to pay the fine the defendant should be arrested and booked into the county jail facility, unless the Municipal Judge is available. If the Municipal Judge is available, the wanted person should be delivered to them for disposition of the warrant. The officer will document the disposition in their warrant arrest report.
- i. The officer should turn in his/her warrant arrest report and the original warrant to his/her supervisor. The supervisor will forward the warrant to the municipal court for a final disposition and removal from the local warrant database.

## VI. ARREST WITHOUT A WARRANT (TEXAS BEST PRACTICES: 7.03)

- A. Federal and state constitutions protect individuals from unreasonable searches. Further, officers must have probable cause to believe that a crime has been committed, and that the person to be arrested has committed the crime.
- B. When warrantless arrests may be made
  1. The Texas Code of Criminal Procedure, in Chapter 14, gives officers the authority to make warrantless arrests, supported by "probable cause," as follows:
    - a. Officers may arrest persons found in suspicious places and under circumstances that establish probable cause that such persons have been guilty of a felony or breach of the peace, or threaten or are about to commit an offense against the laws.
    - b. An officer who has probable cause to believe that a person has committed an

assault resulting in bodily injury to another, and there is probable cause to believe there is danger of further bodily injury to the victim, may arrest that person.

- c. An officer who has probable cause to believe that the person has committed an offense involving family violence may arrest the violator.
  - d. If a person prevents or interferes with an individual's ability to place an emergency telephone call as defined in the Penal Code, an officer may arrest the violator.
  - e. Officers shall arrest a person who violates a valid protective order when the violation is committed in the officer's presence.
  - f. Officers may arrest a person who violates a valid protective order if the offense is not committed in the officer's presence or view.
  - g. Officers may arrest an offender for any offense committed within the officer's presence or view, including traffic violations.
  - h. Officers may arrest at the direction of a magistrate when a felony or breach of the peace has been committed.
  - i. Where it is shown by satisfactory proof to a peace officer, upon the representation of a *credible* person, that a felony has been committed, and that the offender is about to escape, so that there is not time to procure a warrant, said officer may, without warrant, pursue and arrest the accused.
  - j. Officers may arrest a person who confesses to a felony crime, provided the confession complies with state law regarding the admissibility of confessions (TCCP Article 38.21 When Statements May Be Used).
2. Warrantless Arrests Outside Officer's Jurisdiction:
- a. Although officers are discouraged from making arrests outside their jurisdiction, officers may make warrantless arrests in compliance with state law. [Municipal police officers who are outside their jurisdiction may arrest for any offense committed in their presence or view. These officers may only arrest for violations of Subtitle C, Title 7 of the Transportation Code if the violation occurs in the county or counties in which the officer's municipality is located.] Non-municipal Officers who are outside their jurisdiction may arrest, without warrant, a person who commits an offense within the officer's presence or view, if the offense is a felony, breach of the peace, or violation of Chapter 42 or 49 of the Texas Penal Code.
  - b. Any officer making a warrantless arrest outside his/her jurisdiction shall notify the law-enforcement agency of proper jurisdiction. The law-enforcement agency shall take custody of the prisoner and arraign the prisoner before a magistrate in compliance with state law.



## VII. POST-ARREST PROCEDURES

### A. Injury before or during arrest

If a person receives an injury before or during an arrest and either requests medical attention or, in the officer's judgment, medical attention is needed, officers shall transport the suspect or arrange for his/ her transportation to a hospital for an examination before booking.

### B. Processing of paperwork

1. Timely submission of reports is necessary to protect the due process rights of citizens. Officers should immediately produce completed reports for criminal cases. This helps expedite the prosecutorial process and eliminate any due process concerns. To this end, officers of this department shall complete all arrest and booking paperwork before the end of their tour of duty, unless authorized by a supervisor. The arrest and booking paperwork shall be completed immediately upon return to duty if supervisory approval is granted. Supervisory approval may be granted under the following circumstances:
  - a. Call volume taking away the officer's ability to complete the required reports,
  - b. Major crime investigation requiring continued investigative practices employed by this agency,
  - c. Arrest occurring near the end of the officer's tour of duty,
2. Completed reports shall be turned into the submitted reports box for supervisory review and approval. Supervisors will be mindful of reviewing submitted reports and ensure officers complete required reports.
3. Rejected reports are returned to the submitting officer for correction and resubmission for review. Officers receiving a rejected report shall immediately make appropriate corrections and resubmit the report once received.
4. Approved reports are submitted, by supervisors, to the records clerk for processing and routing to the appropriate file or agency for prosecution.

### C. Mirandizing Arrestees

1. Arrestees shall be advised of their Miranda rights before any incriminating questioning is begun.
2. A waiver of the Miranda rights must be obtained before any questioning of an arrestee.
3. If the arrestee has not waived his or her Miranda rights, no questioning shall be conducted beyond that necessary to accomplish the booking procedure (name, address, etc.).

4. If the arrestee declines to waive his or her Miranda right to counsel, or if the arrestee, after waiving that right, elects to reassert it, questioning must cease immediately and no further questioning may be conducted unless:
  - a. An attorney representing the arrestee is present, or
  - b. The arrestee voluntarily initiates a further interview.
5. If the arrestee has not waived his/ her Miranda rights, officers shall refrain from engaging in conversation among themselves in the presence of the arrestee that is calculated to elicit incriminating statements or admissions from the arrestee, even if the conversation does not contain questions.
6. All custodial interrogations of arrested persons shall comply with the requirements found in state law (TCCP Article 38.22).

## **VIII. RELEASE FROM ARREST**

- A. Officers may encounter a circumstance where probable cause develops to arrest a person for an offense only to find out shortly thereafter that the person under arrest did not commit a crime or that the event was not a crime. It is imperative, then, that the officer end the arrest process and release the person as soon as possible. Releasing a person who has been arrested incorrectly is not to be confused with releasing a person who was correctly arrested but is to be released for convenience or medical purposes.

Officers shall consult with supervisors if they are unsure how to handle a situation in which there is a potential for arrest. No officer shall make a decision to arrest a person based on information received from Law enforcement officials outside this agency, nor shall outside officials be consulted for advice on how to handle matters pertaining to cases within our jurisdiction, as they are not privy to the policies and procedures of this agency.

### **B. Procedure**

1. If the arresting officer determines that probable cause no longer exists to arrest a suspect, and the officer is satisfied that the person under arrest either did not commit the crime or that a crime did not occur, the officer shall release the suspect and immediately notify the officer's supervisor.
2. A supervisor, after reviewing facts related with an arrest, determines the officer did not have probable cause to arrest or that a crime was not committed, Shall immediately take steps to have the arrested person released without delay.
3. An officer who releases a subject from arrest shall return the person to the place of the arrest if the location is safe. The officer shall not release the person along the roadside. If a vehicle has been towed, the vehicle shall be returned to the operator/registered owner unless it is required as evidence, or some other legal authority assumes custody of the vehicle.

4. Upon releasing a person in this manner, the officer shall immediately contact a supervisor and advise him/her of the incident.
5. The officer shall document the following in an incident report:
  - a. The date and time of arrest.
  - b. The person arrested (name, address, date of birth, race).
  - c. The location of arrest.
  - d. Probable cause for the arrest and the specific charge(s).
  - e. The location and time of release from arrest and whether the person was transported.
  - f. The reasons or discovery of information that led the officer to release from arrest.
  - g. Any witnesses to the alleged crime, or to the fact the person arrested was allegedly involved.
  - h. Whether force was used in making the arrest, and if so, the nature of the force used and the consequences, including medical aid.

## **IX. IMMUNITY FROM ARREST**

### **A. Legislative immunity**


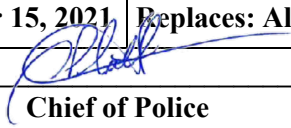
1. Members of the United States Congress are exempt from arrest when Congress is in session, or when they are in route to or from congressional business, except for traffic summonses.
2. Members of the Texas Legislature are exempt from arrest during a legislative session (or allowing for one day for every 20 miles such member may reside from the place where the legislature meets before the beginning or after the ending of any session) except in cases of treason, a felony, or a breach of the peace.

### **B. Diplomatic immunity**

1. While a person claiming diplomatic immunity may present any number of identification papers, the only one that is indicative of the level of privilege and immunity is a card issued by the U.S. State Department. The holder's level of immunity will be indicated on the card. If a person claiming immunity does not possess this card and the incident involves a criminal offense, officers may detain the person either at the scene or at the department long enough to verify official status.
2. Upon exhibiting proof of diplomatic immunity, persons shall be released upon being stopped for a misdemeanor traffic violation. If questions arise about this procedure, or

if an arrest for a felony is necessary, call and advise the U.S. State Department Office of Security (202-647-4415, days, or 202-647-1512, nights and weekends).

3. When encountering a criminal suspect who claims diplomatic immunity, officers shall first take reasonable measures--including pat-downs or other legal searches--to ensure safety to the public and other officers. Verification of the diplomatic claim shall take place after any danger has been neutralized. A criminal investigation shall proceed as if no valid diplomatic immunity claim has been made. Interviews, interrogations, seizures of evidence, or issuance of warrants shall proceed per departmental procedure. In a criminal investigation, the Chief shall remain in contact with the U.S State Department.
  
4. Regardless of the claim of immunity, in any case where officers arrest or detain foreign nationals the suspects shall be advised of their right to have their consular officials notified. In some cases, this notification is mandatory. Note: The list of countries that require mandatory notification of consular officials if one of its citizens has been arrested is extensive. The State Department shall be contacted for guidance. (TEXAS BEST PRACTICES 10.22)

	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 7.3 Search Incident to Arrest and Other Searches Without a Warrant</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____ <div style="text-align: center; margin-left: 150px;">   <b>Chief of Police</b> </div>
	<b>Reference:</b> TEXAS BEST PRACTICES: 7.07, 10.14, and 10.15

## I. POLICY

To ensure that constitutional rights are protected, officers will obtain search warrants upon probable cause in all appropriate criminal cases except for the following circumstances detailed in this policy. (Search warrants are discussed under Policy 7.5.)

Searches without a judicial warrant are strictly limited to those circumstances where the courts have granted officers limited exceptions. One of those exceptions was described in Policy 7.2, where, if during an investigative stop (detention), an officer has reasonable suspicion that an individual may be armed, and is able to articulate that suspicion, the officer may conduct a limited pat-down of the individual's outside clothing to protect the officer. Other exceptions to the search warrant requirement are provided in this policy.

## II. PURPOSE

The purpose of this policy is to establish guidelines for searches incident to arrest and other searches without a warrant.

## III. SEARCH INCIDENT TO LAWFUL ARREST

- A. The general rule is that a reasonable search may follow a valid arrest. The officer has the authority to make a search that may extend to articles carried by the suspect and to the suspect's immediate surroundings. The purpose of this search is to remove any weapons from the arrested person that could be used against the officer while in custody, to remove any items that might facilitate an escape, and to prevent the destruction of any evidence by the arrested person.
- B. A search incident to an arrest must occur in such a way that it and the arrest are part of a continuous, uninterrupted transaction. Two conditions are necessary for this to occur:
  1. The search must be made as soon as practical after the arrest.
  2. The search must be made at or near the place of the arrest.

- C. An officer making a search incident to an arrest may search only the following places:
1. The entirety of the person being arrested.
  2. The areas within the wingspan or physical arm's reach of the person being arrested where the suspect might reach for a weapon or for evidence.
- D. Accessories, such as a purse or a backpack, carried by the suspect may be searched incident to a full custodial arrest for they are within the area in which the defendant might reach to grab a weapon or an item of evidence.
- E. Vehicles may be searched contemporaneous with the arrest of the occupant or driver only in the following circumstances:
1. The arrested vehicle occupant is unsecured and within arm's reach of the passenger compartment at the time of the search and the officer can articulate a safety concern, or
  2. The officer has a reasonable belief that evidence related to the crime for which the arrest was made is located within the passenger compartment.
  3. Once an occupant has been arrested and secured and is unable to effectively reach the passenger compartment, the authority to search the vehicle for safety reasons is removed.
- F. Strip searches
1. Strip searches shall not be conducted of persons arrested for traffic violations, or for Class C or B misdemeanors unless the officer has an articulable, reasonable suspicion that the person is concealing a weapon or contraband. Reasonable suspicion may be based on, but is not limited to, the following criteria.
    - a. Nature of the offense.
    - b. Arrestee's demeanor and appearance.
    - c. Circumstances of the arrest or evidence of a major offense in plain view or during the arrest.
    - d. Arrestee's criminal record, particularly a history of violence or of narcotics offenses.
    - e. Detection of suspicious objects beneath the suspect's clothing during a search incident to an arrest.

2. Strip searches shall be performed by persons of the same sex as the person arrested and at the jail or lock-up where the search cannot be observed by persons not physically conducting the search.
3. No strip searches will be conducted in the field.
4. In every case, the on-duty or on-call supervisor must review the need and expressly authorize the strip search.
5. When authorized by the supervising authority, strip searches may be conducted only under the following conditions:
  - a. In conformance with approved hygienic procedures and professional practices.
  - b. In a room specifically authorized for this purpose.
  - c. By the fewest number of personnel necessary and only by those of the same sex.
  - d. Where conditions provide privacy from all but those authorized to conduct the search.
6. Following a strip search, the officer performing the search shall submit a written report to the supervisory authority that details, at a minimum, the following:
  - a. Date and place of the search.
  - b. Identity of the officer conducting the search.
  - c. Identity of the individual searched.
  - d. Those present during the search.
  - e. The identity of the approving supervisor.
  - f. A detailed description of the nature and extent of the search.
  - g. The results of the search.

#### G. Body-cavity searches

1. Department personnel do not conduct body cavity searches other than an individual's mouth. If an officer has reasonable cause to believe a body-cavity search is needed to detect weapons, drugs, or other contraband, the following procedures apply:
  - a. The on-duty or on-call supervisor is notified.

- b. A search warrant is secured.
  - c. The detainee is transported to an appropriate medical facility.
  - d. The search is conducted by the on-duty emergency room physician, while officers stand by to take control of any evidence and provide security to the physician conducting the search.
  - e. Body cavity searches are documented in the officer's arrest report, which will detail the officer's justification for such search, the approving supervisor's name, the location and persons present during the search, and the results of the search. A copy of the report and the warrant are forwarded to the Chief of Police for review and filing.
2. Prior to transporting the prisoner to the medical facility, the officer shall inform the prisoner of his or her intention to conduct a body-cavity search, thus giving the prisoner the opportunity to voluntarily surrender the suspected contraband.

#### **IV. CONSENT SEARCH**

##### **A. Consent Searches**

A search warrant is not necessary where a person who has authority or control over the thing or place to be searched consents to the search. Note that the officer is not required to have reasonable suspicion or probable cause to request a consent search. He or she may merely ask for permission from someone with control over the item or premises. If that person grants permission, the search may take place. The sole justification for a consent search is the existence of knowing, intelligent, and voluntary consent.

1. Consent searches must observe the following rules:
  - a. Generally, the person granting consent must use, access, or control the property. A person having use, access, or control of only a part of a jointly owned property can give consent for a search only of that part.
  - b. If two people have joint ownership of property, either may give consent where only one of the owners is present. If possible, officers should have all the consenting parties' present sign a written permission-to-search form.
  - c. If both or multiple parties with joint ownership are present and any party refuses to consent to the search, the search cannot be performed.
  - d. A landlord, including a hotel or motel manager, cannot consent to a search of a tenant's premises unless the tenant has been evicted or has abandoned the property.



- e. A husband or wife, or one member of a cohabiting unmarried couple, may consent to a search of areas in common ownership or use where only one is present. If both or multiple parties with joint ownership are present and any party refuses to consent to the search, the search cannot be performed.
  - f. A parent may consent to a search of premises occupied by a child under the age of majority if the parent also has access to the premises. If a dependent child is present and is over the age of majority, he or she may legally object to the search of an area that is jointly owned or possessed.
  - g. An employee cannot give valid consent to a search of his/her employer's premises unless he/she has been left in custody of the premises.
  - h. An employer may generally consent to a search of premises used by employees, except premises used solely by another employee (e.g., a locker).
  - i. Consent must be given voluntarily. If an officer requests consent from a person under circumstances which a reasonable person would consider coercive, the search would not be consensual, and the officers should seek a warrant. The officer has the burden of demonstrating that the consent was given voluntarily.
  - j. A person who initially gives consent may withdraw it at any time. Officers shall then secure the premises and seek a warrant if probable cause exists.
  - k. Refusal to give consent cannot justify further law-enforcement action.
  - l. The scope of a consent search is limited to the area for which consent has been given, and within this area officers may search only into areas where the objects sought could reasonably be hidden.
2. Documentation of Consent Searches
- a. Although verbal consent is valid, police officers will carry and use the Voluntary Consent to Search form. The form should be completed and signed by the consenting parties. All Consent to Search Forms shall be forwarded to the records unit for filing, attached with the submitted report detailing the search.
  - b. If a person gives verbal consent but refuses to give written consent, police officers should consider the severity of the case along with viable options (e.g., obtaining a search warrant or some other exception to the search warrant requirement) before proceeding with the search.

- c. A police officer who is equipped with a body camera or dash camera shall record the request for consent and the person's response. The recording shall be preserved as evidence, should evidence or contraband be discovered or other enforcement action result from the search.
- d. A police officer who proceeds to search on verbal consent should remember that the burden of proof is always on the government.
- e. Police officers will not only have to prove the consent was voluntary, but that it was given (officer's word against defendant). Officers should attempt to take additional steps to eliminate this argument. For example, they could have an impartial third party witness the consent by signing the form.
- f. Police officers should make every effort to minimize conditions that could be offered as "threat or intimidation," such as the following:
  - i. Number of police officers present (especially in uniform)
  - ii. Amount of force used to detain or arrest, e.g., displaying firearms, use of handcuffs, etc.
  - iii. Language and tone of voice used in requesting consent
  - iv. Other non-verbal communications.

## **V. EMERGENCY SEARCH**

- A. An emergency search is a search in which an officer makes a warrantless nonconsensual entry into a residence or building to protect someone's life or render emergency life-saving assistance to an occupant. This search is not based in criminal law enforcement principles; rather it is to save life. Examples of emergency searches include, but are not limited to:
  - 1. Fire
  - 2. Shouts for help
  - 3. Unconscious person
  - 4. Welfare checks, if the information known to the officer gives rise to a reasonable concern for the well-being of an occupant
  - 5. Sounds of a fight coming from inside the residence
- B. Officers should understand that once entry is made, and the emergency has been rendered safe his or her authority to be in the residence has expired. Additionally, entry pursuant to an

emergency does not then give the officer authority to search the residence for evidence of a crime.

- C. The test for the validity of an emergency search will be whether a reasonable officer, under the same circumstances, would have believed there was a threat to life or limb of an occupant.

## **VI. MOTOR VEHICLE SEARCH BASED ON PROBABLE CAUSE**

- A. In recent years, the U.S. Supreme Court has modified and expanded the conditions under which officers may search vehicles. Preferably, officers shall search vehicles under the authority of a warrant, although it often happens that there is not sufficient time to obtain one. However, warrantless searches of vehicles may take place under varying conditions and circumstances. It is imperative that officers understand the different types of vehicle searches and their limitations.

NOTE: With a warrant, a search may extend anywhere within the vehicle unless the warrant itself imposes limits.

### **B. Definitions**

1. For the purposes of this section, a motor vehicle is any vehicle operating or capable of being operated on public streets or highways, from trucks to automobiles to mobile homes. A vehicle that has been immobilized in one location for use as a storage facility or home is not a motor vehicle for fourth amendment purposes.
2. For the purposes of this section, a search is an examination of a motor vehicle with an investigative motive, that is, to discover evidence or to examine the vehicle identification number (VIN) to ascertain ownership.

A motor vehicle may be searched without a warrant if the following conditions are present:

- a. The officer has probable cause to believe the motor vehicle is being used to transport contraband
- b. The motor vehicle is mobile or readily mobile

The scope of a motor vehicle search is the entire motor vehicle, including containers in the motor vehicle in which the suspected contraband could fit.

If contraband is located by way of a lawful frisk or search of an occupant of the motor vehicle, the officer may rely upon this as probable cause to search the motor vehicle for additional contraband. The reverse is not the case. The discovery of contraband in a motor vehicle will not automatically authorize a search of the

occupants of the motor vehicle. Officers must be able to articulate individualized probable cause to search the occupants.

An entry into the vehicle to examine the VIN or otherwise determine ownership must be limited to those purposes.

An emergency search of the vehicle may be conducted but the extent of the search must not exceed whatever is necessary to respond to the emergency.

Note: If the initial search under the above conditions gives rise to probable cause that evidence, contraband, fruits of a crime, or instrumentalities of the crime might be found elsewhere in the vehicle, officers may search those areas that might reasonably contain such items.

### C. Containers within the vehicle

1. As a rule, no container within a vehicle shall be searched unless it might contain the item(s) sought.
2. Procedures for unlocked containers
  - a. In a probable cause search, containers may be opened wherever found in the vehicle.
  - b. When the passenger area is searched incident to an arrest, containers within the passenger area may be opened.
  - c. During a consent search, containers may be opened provided that the terms of the consent either permit the search or reasonably imply permission.
  - d. Containers found in or discarded from a vehicle under circumstances not amounting to probable cause or in connection with a search incident to an arrest shall not be searched but shall be secured until a warrant is obtained.
  - e. The abandonment doctrine does apply to containers thrown from a vehicle by a suspect.
3. Procedures for locked containers
  - a. Under most conditions, locked containers shall be opened under a warrant unless one of the following circumstances has been met:
    - i. Consent has been given.

- ii. Probable cause exists to search the vehicle and the object of the search might be found in the container. (Even in this circumstance, a warrant is preferred.)
- iii. Inventory, only if a key is present.

#### D. Conduct of the vehicle search

1. When possible, searches of vehicles shall be conducted contemporaneously with the stopping or discovery of the vehicle. Generally, vehicle searches shall be conducted as soon as reasonably possible.
2. When possible, officers shall avoid damaging a vehicle or its contents, and shall minimize the intrusiveness of the search and any inconvenience suffered by the passengers or owner.

As vehicles may contain sharp or pointed objects, and perhaps even syringes or other materials with body fluids on them, officers shall take precautions to minimize exposure to communicable diseases.

### **VII. INVENTORY OF A MOTOR VEHICLE**

When an officer has decided to lawfully impound a motor vehicle the officer shall inventory the contents of the motor vehicle. An inventory is not considered a search – it is an administrative caretaking procedure to protect to department from false claims and safeguard property.

Officers shall follow policy 7.16 when impounding motor vehicles.

### **VIII. FRISK**

#### A. PERSONS:

A frisk is a limited search for weapons. A frisk, by definition, occurs during a lawful detention. Officers shall not frisk a person during a consensual encounter unless the circumstances escalate to the point where the officer has reasonable suspicion to detain and can articulate a fear for his or her safety. A frisk of a person during a consensual encounter will most likely turn the consensual encounter into a seizure. Officers should conduct a full search of a person who has been arrested.

Officers do not have the authority to automatically frisk a person who has been detained. Officers shall articulate and document specific facts and circumstances that caused the officer to fear for her or his safety.

A frisk is conducted by patting down the outer clothing for weapons. If an officer detects contraband during a frisk the officer may proceed under the plain touch doctrine.

## B. MOTOR VEHICLES

A motor vehicle may also be frisked. The following requirements must be met:

1. It must be a lawful detention
2. Facts and circumstances must be present to cause a reasonable officer to fear for her or his safety from an occupant of the vehicle
3. The occupant causing the concern must be frisked first
4. The officer must intend to release the detainee and allow the person back into the car, e.g. a traffic citation as opposed to an arrest
5. The officer may frisk the area in the passenger compartment that is immediately accessible to the detained person once returned to the vehicle.

## IX. PLAIN TOUCH

- A. The plain touch doctrine authorizes an officer to go into a detainee's pocket to retrieve contraband if the officer detects the contraband through the sense of touch during a lawful frisk.
- B. Extensive manipulation of the item to ascertain its nature is not permitted and does not follow the guidelines for the plain touch doctrine.
- C. If the officer detects a solid container of some sort the plain touch doctrine does not authorize the officer to open the container to ascertain its contents. The officer will have to have another search warrant exception or consent to open the opaque container.

## X. IMMINENT DESTRUCTION OF EVIDENCE

- A. An officer is authorized to make a warrantless, nonconsensual entry into a residence or building to prevent the imminent destruction of evidence:
  1. It must be the type of evidence that can be easily lost or destroyed
  2. The destruction of the evidence must be imminent
  3. The attempted destruction cannot be prompted by police misconduct
- B. Once the evidence that was the subject of the attempted destruction is secured officers shall secure the residence and obtain a search warrant to search the residence for additional evidence or contraband.

## **XI. ENTRY INTO A RESIDENCE TO EFFECT ARREST**

Both state statutes and federal case law regulate entry to make an arrest. The primary focus of any entry to make an arrest is the safety of the officers executing the warrant and the occupants of the residence. Knocking on the door affords the occupants time to answer the door and comply with the officer's orders.

### **A. WITH ARREST WARRANT**

Officers may force entry to execute an arrest warrant subject to the following rules:

1. Felony warrant
2. Officer is entering the residence where the person named in the warrant resides
3. Denied admittance after knocking and announcing
4. Knocking and announcing may be waived under the following circumstances: knocking and announcing will prompt an escape attempt, place the officer(s) in danger, or the suspect is already aware of the officer's presence.

### **B. WITHOUT ARREST WARRANT – SUSPECT OBSERVED OUTSIDE RESIDENCE**

When officers observe a dangerous felon in a public place and are authorized to arrest without a warrant, officers may pursue and force entry into a residence to arrest the dangerous felon without an arrest warrant. The following requirements must be met:

1. The offense must be a dangerous felony. A dangerous felony can best be characterized as one that involves a component of violence or threatened violence
2. The officer must already have probable cause to effect the arrest
3. There must be a true exigency to justify the entry e.g. escape, danger to occupants or others.

### **C. WITHOUT ARREST WARRANT – OFFENSE OCCURS INSIDE RESIDENCE WITHIN OFFICER'S VIEW**

1. Police officers who observe criminal activity occurring inside a private place from outside the private place may not always be able to secure a proper warrant in a timely manner and will adhere to the following guidelines:
  - a. If the offense is a misdemeanor, police officers will not enter except under the following circumstances:

- i. Valid consent is given by a person with authority to grant such permission and who lives at the residence.
  - ii. There is reason to believe someone inside the residence is in immediate danger of life or limb
  - iii. The officer reasonably believes the destruction of contraband or other evidence is imminent if it is not immediately recovered.
- b. If the offense is a felony, police officers will not enter except under the following circumstances:
- i. Valid consent is given by a person with authority to grant such permission and who resides at the location.
  - ii. The officer reasonably believes the destruction of contraband or other evidence is imminent if it is not immediately recovered.
  - iii. There is reason to believe someone inside the residence is in immediate danger of life or limb.

## **XII. PLAIN VIEW**

A plain-view seizure is, technically, not a search. To make a plain-view seizure of property, such as contraband, fruits of a crime, or instrumentalities of a crime, the following two requirements must be met:

- A. From a lawful vantage point, the officer must observe contraband left in open view.
- B. It must be immediately apparent to the officer that the items he or she observes may be evidence of a crime, contraband, or otherwise subject to seizure.

## **XIII. OPEN FIELDS, CURTILAGE, ABANDONMENT**

A search warrant is not required for property that has been abandoned.


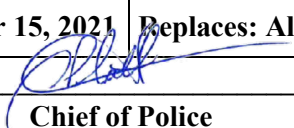
- A. For property to be considered abandoned the following conditions must apply:
  1. The property was voluntarily abandoned.
  2. The abandonment was not a result of police misconduct.



B. Open fields are not protected by the Fourth Amendment, but officers must distinguish them from curtilage, searches of which require a warrant. Curtilage is the area of a dwelling that is necessary, convenient, and habitually used by the family for domestic purposes. The extent of curtilage of a private residence is determined by the following:

1. Whether the area is enclosed, but an enclosure is not required to establish curtilage.
2. The nature and use of the area.
3. The proximity of the area to the home.

Note that under some circumstances surveillance (e.g., aerial surveillance) of activities within curtilage may take place without a warrant.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.4 Search Warrants</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b>	 <b>Chief of Police</b>
<b>Reference: TEXAS BEST PRACTICES: 7.06</b>		

## I. POLICY

Both federal and state constitutions guarantee every person the right to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. U. S. Supreme Court decisions regarding search and seizure place the responsibility on the police to ensure that every person’s fourth amendment rights are protected.

Officers shall scrupulously observe constitutional guidelines when conducting searches, and they will always remain mindful of their lawful purpose. Unlawful searches can result in harm to members of the community, put officers at risk, and possibly damage the department’s image in the community.

Search warrants are one of the most valuable and powerful tools available to law-enforcement officers. Officers of this department shall have a thorough knowledge of the legal requirements involved in obtaining and executing search warrants.

## II. PURPOSE

The purpose of this policy is to establish guidelines and procedures that officers must follow when conducting searches and seizures.

## III. DEFINITIONS

- A. Search Warrant: A written order, issued by a magistrate and directed to a peace officer commanding him/her to search for a particular item or person and to seize the same and bring it before such magistrate, or commanding him/her to search for and photograph a child and deliver to the magistrate any of the film exposed pursuant to the order. Search warrants are also issued for biological specimens and seizure of a person, pursuant an arrest warrant.
- B. Search Site: The premises to be searched, as explicitly stated in the search warrant.
- C. Lead Officer: The officer primarily responsible for the investigation that will prepare, plan, and implement the search warrant.

- D. Protective Sweep: A quick and limited search of premises incident to an arrest or service of an arrest warrant performed to locate other persons inside who might pose a risk to the officers. Officers must be able to articulate a reasonable basis their safety concerns.
- E. Curtilage: Curtilage usually refers to the yard, garden, or any piece of ground that is immediately adjacent to a premise and is used as part of the activity of the premises. While the term has no absolute definition that applies under all circumstances, the curtilage of a private residence, for instance, may be defined by the size of the lot on which the dwelling stands, whether the area around the dwelling is enclosed, the nature and use of the area, the proximity of the area to the home, and any measures taken by the owner to protect the area from observation.

#### **IV. PROCEDURES - General**

##### **A. State Law**

- 1. Chapter 18 of the Texas Code of Criminal Procedure controls the use of search warrants in Texas. It states that a judge or magistrate may issue a search warrant if the following circumstances exist:
  - a. There is probable cause to do so, and
  - b. There is a complaint on oath supported by an affidavit.
- 2. Search warrants may be issued for the search of specified places, things or persons, and seizure therefrom of the following things as specified in the warrant:
  - a. Weapons or other objects used in the commission of a crime.
  - b. Articles or things the sale or possession of which is unlawful.
  - c. Stolen property or the fruits of any crime.
  - d. Any object, thing, or person, including documents, books, records, paper, or body fluids constituting evidence of a crime.

Please see the applicable statutes for a more comprehensive listing.

##### **B. Supreme Court Decisions**

- 1. The Supreme Court of the United States issues decisions that must be used as guidelines in conducting searches. Because the fourth amendment to the Constitution prohibits unreasonable searches and seizures, officers bear the burden of proving that the search is reasonable. The court will examine reasonableness based on the answers to these questions:
  - a. Was there probable cause to issue the search warrant?

b. Was the scope of the search appropriate?

C. Exceptions to search warrant requirements are discussed in Policy 7.4.

## **V. PROCEDURES: Obtaining a Search Warrant**

A. Prior to obtaining a search warrant, officers should consult a departmental supervisor for review of the probable cause and for approval to seek a search warrant. This review may be conducted by telephone if necessary. If the supervisor approves the warrant application, the supervisor shall notify the Chief of Police immediately and inform the Chief of the circumstances surrounding the offense and the need for the warrant.

B. The approving supervisor will oversee the warrant execution. While the lead officer may develop the case information, construct the affidavit, obtain the warrant, and seek assistance from outside agencies if needed, the approving supervisor is responsible for the proper and safe execution of the warrant, including compliance with this policy.

C. Essential legal requirements

1. To obtain a search warrant, an officer must show probable cause to believe that specific evidence, contraband, or fruits of a crime may be found at a location.
2. The officer shall prepare an affidavit that carefully documents specific facts that constitute probable cause. Two kinds of facts must be considered:
  - a. The facts from which the officer concluded that the person or thing is probably located at the place to be searched.
  - b. The facts that address the reliability of the source of the officer's information.
  - c. The information upon which the officer relies is not stale, within the context of the offense being investigated.
3. The court considers only those facts presented in the affidavit.
4. Conclusions and suspicions are not facts.
5. Apart from the officer's personal knowledge or observations, facts may derive from a reliable informant.
6. Reliability of facts is established by the following:
  - a. Personal observation or knowledge possessed by an officer.
  - b. Witnesses who have knowledge of information pertinent to the case.
  - c. Informants if they have proven to be reliable or if their information is corroborated by personal observation of an officer.

#### D. Affidavits

1. The accuracy of the affidavit is vital to the validity of the search warrant. TCCP Article 18.01 requires officers to swear to the facts of the affidavit before a judge or magistrate.
2. The affidavit shall include the following elements:
  - a. A detailed description of the place, thing, or person to be searched.
  - b. A description of the things or persons to be seized pursuant to the warrant
  - c. A substantial allegation of the offense in relation to which the search is to be made.
  - d. An allegation that the object, thing, or person to be searched or searched for constitutes evidence of the commission of the offense.
  - e. Material facts that would show that there is probable cause for issuing the search warrant.
  - f. Facts that establish probable cause and that the item or person to be seized is at the location to be searched.

#### E. Language of the warrant

1. Only the things specified in the search warrant can be seized. (For a discussion of exceptions to this, such as plain-view seizures and searches incident to arrest, see Policy 7.4).
2. The warrant shall precisely state the areas to be searched.
3. If officers wish to search a home and its surroundings, the affidavit must specify a "premises" search and its curtilage, and must identify all outbuildings, such as garages or tool sheds, as appropriate.
4. If motor vehicles to be searched are on the premises, the warrant shall so specify.
5. If searches of specific persons (other than frisks) are to be included during the search, the warrant shall so specify. If the warrant states that all person's present shall be searched, probable cause to do so must be stated in the affidavit.
6. The items to be searched for shall be precisely described. If an item to be searched for may be dismantled (e.g., firearms), the warrant must specify the search for parts, pieces, or components of the item.

7. If officers anticipate searching for and seizing computers or similar complex technological items, experts must be consulted to determine the appropriate language to list in the affidavit and for outlining appropriate guidelines in the warrant for seizure of hardware and software.
8. The affidavit and warrant should be reviewed by the county attorney prior to presenting it to a magistrate.
9. If officers believe it is in the best interest of officer safety or that evidence may be destroyed if advanced warning is given and wish to utilize a “no-knock” warrant execution, the reasons for that belief should be clearly explained in the affidavit. The magistrate should be requested to review and authorize the no-knock entry.

## **VI. PROCEDURES: Executing a Search Warrant**

### **A. When a search warrant must be executed**

1. An officer is required to execute a warrant within the limitations imposed by statute (TCCP Article 18.06). If it has not been executed during that time, the officer shall void the warrant and return it to the magistrate who issued it.
2. An officer may execute a search warrant either during the day or at night. The time of day selected to execute the warrant should take into consideration the likelihood that a specific category of individuals will or will not be present, e.g., children or elderly. Officer safety will also be considered in determining when to execute a warrant.

### **B. Preparing to execute the warrant**

1. Before executing the warrant, the on-duty supervisor shall review the warrant and the affidavit and brief the search team officers on the procedures to be followed. The supervisor shall ensure that the entire warrant process is documented. Written reports shall be supplemented with photographs or videotape, if available and appropriate.
2. All members of the search team shall be in uniform or wear a clearly marked jacket or ballistic vest with “POLICE” in large letters on the front and back.
3. All members of the search team shall wear protective body armor during the execution of all warrants.

### **C. Gaining entrance to premises**

1. Prior to execution of the warrant, the lead officer shall attempt to determine if any circumstances have changed that make executing the search warrant undesirable at that time. Where possible, pre-search surveillance shall be conducted up to the point at which the warrant is executed.
2. The lead officer shall make a final assessment of the accuracy of the warrant in

relationship to the location to be searched.

3. The search team shall first deploy around the premises to be searched, ensuring that all exits are covered.
4. Uniformed officers shall be the most visible members of the search team and shall conduct the initial entry.
5. In most cases officers shall do all the following before entering the premises to be searched:
  - a. He/she must announce his/her presence as a law-enforcement officer.
  - b. The officer must announce that his/her purpose is to execute a search warrant.
  - c. The officer must wait a reasonable time either to be admitted or refused admission to the premises unless a “No Knock” entry provision has been made by a magistrate on the search warrant.

6. When entrance is refused:

An officer who is refused entrance after a reasonable time may force his/her way into the premises using only that force which is applicable to the circumstances. “Reasonable time,” in this context, depends on the circumstances. A refusal may be expressed or implied.

- a. No one has admitted the officer within a time that a reasonable person would expect someone to let the officer in if he or she is going to be admitted at all.
  - b. The officer waiting to be admitted sees or hears suspicious circumstances, such as flushing toilets or footsteps running away from the door, which indicate that someone might be concealing or destroying evidence or trying to escape.
7. No-knock or exigent entry:

In some circumstances a police officer may enter the premises to be searched without announcing his or her presence and purpose before entering. The judicial authority issuing the warrant may add a no-knock entry provision to the warrant. If not, the decision to make a no-knock entry may be made by the on-scene supervisor based on facts that would lead him or her to believe that an announcement would result in one of the following:

- a. Bodily harm either to the officer or to someone within the premises to be searched.
- b. The escape of the person to be searched or arrested.
- c. The destruction of evidence.

8. If circumstances require a no-knock or exigent entry, the first officer to cross the threshold into the premises shall announce that law-enforcement officers are executing a warrant. To ensure their own safety officers shall command the occupants to take appropriate action, such as "police, search warrant, get down."

#### D. Conduct of the search

1. Upon entry, after all occupants have been secured, the occupant shall be given a copy of the search warrant. A copy of the search warrant, along with an inventory of items seized, shall be left in a conspicuous place if no persons are present when execution of the search warrant is completed.
2. The supervisory officer shall ensure that a protective sweep of the site is performed immediately.
3. After the site has been secured, a photographic and/or videotape record of the premises shall be made prior to conducting the search.
4. The search must cease when all the evidence being searched for is located.
5. Officers should exercise reasonable care in executing the warrant to minimize damage to property. If damage occurs during an entry to premises that will be left vacant, and the damage may leave the premises vulnerable to security problems, arrangements shall be made to guard the premises until it can be secured or turned over to a responsible person with authority over the property.
6. If damage occurs, justification for actions that caused the damage and a detailed description of the nature and extent of the damage shall be documented. Photographs of the damage should be taken where possible.
7. Officers causing damage shall not obligate the City of Teague or the police department to repair any damages incurred in this process, nor shall any officer offer to, or refer someone, repair the damages.
8. Officers shall not use a search warrant to conduct a fishing expedition, i.e., if the search warrant is for a large item, such as a television set, small places, such as jewelry boxes, may not be searched.
9. An officer may seize only the property listed in the warrant with two exceptions:
  - a. The other evidence is reasonably related to the offense for which the search warrant was issued.
  - b. It is property that the officer knows or has probable cause to believe is evidence of another crime.
10. Currency taken as evidence shall be verified by a supervisor and transported to a safe or secured in an evidence locker at the police department.



11. If items are taken from the search site, an itemized receipt shall be provided to the resident/occupant, or in the absence of the same, left in a conspicuous location at the site.

E. Searches of persons found on premises

1. A person's presence on the premises to be searched with a warrant does not, without more evidence than the person's mere presence, give rise to probable cause to search that person beyond a frisk for officer safety.
2. A warrant to search the premises for contraband does carry with it the authority to detain the occupants of the premises while a search is being conducted. If the search of the premises gives rise to probable cause to arrest the detainee, he or she may be arrested and his or her person searched incident to arrest.
3. A person on the premises may be searched if the officer has probable cause to believe that items listed in the warrant are concealed on the person.
4. If an officer determines a frisk is necessary, the officer must articulate the facts present that justify the frisk of the person.

**VII. PROCEDURES: High-risk warrant execution**

- A. A high-risk warrant is requested for any situation where it is likely that any special obstacle to the safe, effective execution of the warrant is present, the location has been fortified, or officers may meet armed resistance or other deadly force. This suspicion should be corroborated by intelligence information, for example, information from Computerized Criminal History (CCH), Confidential Informant/Cooperating Individual (CI), statements, history of location, or the officer's personal knowledge.
- B. High-risk search warrants will utilize SWAT (or the appropriate tactical unit within the jurisdiction) for entry and the securing of the premises.
- C. The supervisor in charge of executing the warrant will notify the SWAT commander through the proper channels and will provide a copy of the warrant and the affidavit.
- D. Upon notification by any supervisor that SWAT will be needed to execute a warrant, the SWAT commander will contact the lead officer and obtain the details of the warrant execution. This will include a physical inspection of the target, verification of the address, and a physical description.
  1. Upon completion of the scouting report, together the lead officer, supervisor, and the SWAT commander will formulate a plan of execution.
  2. The SWAT commander, based on their policies or interlocal agreements in force, will notify the number of SWAT officers required and tell them when and where they are to report.

3. Use of on-duty patrol officers should be coordinated with the on-duty supervisor to avoid depleting manpower.
- E. A warrant execution briefing will be held. The warrant execution briefing will be conducted by the lead officer, supervisor, and the SWAT commander. It will include the supervisor in charge of executing the warrant, Emergency Medical Services, and all other officers participating in its execution or who will be at the scene. If this is a joint agency task force operation, officers from the participating agency will be present and identified as members of the warrant service team.
1. Lead officer and the SWAT commander will lay out in detail the procedures for executing the warrant to all team members. The plan will include but not necessarily be limited to the following:
    - a. The specific items subject to the search as defined in the warrant, and any available information on their location.
    - b. Information concerning the structure to be searched and surroundings, to include floor plans where available, mockups, photos, and diagrams of the location identifying entrances, exits, obstructions, fortifications, garages, outlying buildings, suspect vehicles, and all other points of concern.
    - c. Identification of suspects and other occupants who may be present at the location—incorporating photos or sketches whenever possible—with emphasis on suspect threat potential, as well as the presence of children, the elderly, or others who may not be involved with suspects.
    - d. A complete review of the tactical plan to include the staging area, route of approach, individual assignments for entry, search, management of evidence, custody and handling of seized vehicles, custody of prisoners, and post-execution duties, such as securing the location and conducting surveillance on the site for additional suspects.
    - e. Listing personnel resources and the armament necessary for gaining entry, for the safety and security of officers, or for conducting the search.
    - f. Contingency plans for encountering hazardous materials, canines, booby traps, fortifications, or related hazards.
    - g. Measures to take in case of injury or accident, to include the nearest location of trauma or emergency care facilities.
    - h. Procedures for exiting the location under emergency conditions.
  2. The entry team shall always include uniformed officers who shall be conspicuously present at the place and time the warrant is served. All non-uniformed officers shall be clearly identified as law-enforcement officers by a distinctive jacket, ballistic vest, or some other conspicuous indicator of office.

3. All members of the search team shall wear body armor or ballistic vests as designated by the supervisor.
4. Prior to execution of the warrant, the lead officer shall attempt to determine if any circumstances have changed that make executing the search warrant undesirable at that time.
5. Where possible, pre-search surveillance shall be conducted up to the point at which the warrant is executed.
6. The lead officer shall make a final assessment of the warrant's accuracy in relationship to the location to be searched.
7. The lead officer shall ensure that the entire search warrant execution process is documented from the beginning until the search team leaves the premises. This written record shall be supported by photographs and, if practical, videotaping of the entire search process.

#### F. Entry Procedures

1. If an advance surveillance team is at the target site, radio contact shall be made to ensure that the warrant can be served according to plan.
2. The search personnel shall position themselves in accordance with the execution plan.
3. An easily identifiable police officer shall knock and notify persons inside the search site, in a voice loud enough to be heard inside the premises, that he or she is a police officer and has a warrant to search the premises, and that he or she demands entry to the premises at once.
4. Following the knock-and-announce, officers shall delay entry for an appropriate period of time based on the size and nature of the target site and time of day to provide a reasonable opportunity for an occupant to respond (normally between 15 and 20 seconds), unless a "No Knock" provision has been issued by the magistrate. If there is reasonable suspicion that the delay would create a high risk to the officers or others, inhibit the effectiveness of the investigation, or permit the destruction of evidence, entry may be made as soon as practicable.
5. Once the entry has been made and the scene secured, the lead officer will perform the search as required in Section VI. D above.


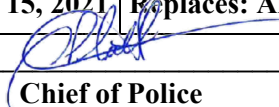
### VIII. PROCEDURES: Return of the search warrant

- A. An officer who has finished a search shall perform the following:
  1. Note the date and time of execution on the search warrant.

2. Make an inventory of all the property seized and leave a copy with the person in charge of the premises.
3. Make return of the warrant within three days following the execution of the search (excluding Saturdays, Sundays, and legal holidays) or as otherwise required by statute. The return includes the following:
  - a. The search warrant.
  - b. The affidavit.
  - c. Either the inventory of articles seized or a notation that nothing was seized during the search.

B. Responsibility for property seized

1. Officers must provide a rigorous chain-of-custody procedure for all property seized. Documentation must appear in all narrative reports pertaining to the chain of custody of any items seized. The department evidence tag shall be used to identify all seizures.
2. Officers shall place evidence in the property room or locker reserved for the purpose prior to the end of shift.
3. Officers shall observe the property and evidence procedures as detailed in Policy 12.0.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.5 Limited English Proficiency</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b>	

## I. POLICY

Our country has always been a melting pot of cultures. Throughout our history, individuals with limited English proficiency have found it difficult to clearly understand important rights, obligations, and services. It is, therefore, the policy of this department to take reasonable steps to ensure that all individuals have equal access to the rights, liberties, and services of government, regardless of their national origin or their primary language. (Title VI of the Civil Rights Act of 1964, § 601, 42 USC § 2000d)

## II. PURPOSE

The purpose of this policy is to establish direction in dealing with members of the public who have limited English proficiency.

## III. DEFINITIONS

- A. Limited English Proficiency (LEP): This term is used to describe individuals whose primary language is not English and who have a limited ability to read, write, speak, or understand English. LEP individuals may be competent in certain types of communication (e.g., speaking or understanding), but still be LEP for other purposes, such as reading or writing. Similarly, LEP designations are context specific. For example, an individual may possess sufficient skills in the use of English to function in one setting but not in others.
- B. Interpretation: The act of listening to a communication in one language and orally converting it to another language while retaining the same meaning.
- C. Translation: The replacement of written text from one language into an equivalent written text of another language.

- D. Bilingual: The ability to communicate in two languages fluently, including the ability to communicate technical and law-enforcement terminology. For purposes of this policy, employees who are identified as bilingual must initially and periodically demonstrate, through a procedure to be established by the department, a level of skill and competence such that the department is able to determine how their skills can be used.
- E. Authorized Interpreter: An employee or other designated individual who is bilingual and has successfully completed department-prescribed interpreter training and is authorized to act as an interpreter or translator.

#### **IV. FIELD RESPONSE TO LIMITED ENGLISH PROFICIENCY**

##### **A. Identification of an Individual's Primary Language**

1. Officers may encounter individuals in the field who do not clearly understand spoken English. Officers should be alert to clues that will indicate individuals do not clearly understand the officer.
2. An officer who believes an individual does not clearly understand English will utilize all reasonably available tools, such as language identification cards, when attempting to determine an LEP individual's primary language in an effort to avoid misidentifying the language and failing to provide adequate service.
3. Officers needing assistance in communicating with the individual will utilize other options, including the use of signs and gestures, writing notes, or using others at the scene to attempt to communicate with the individual.
4. Except for exigent or very informal and non-confrontational circumstances, the use of an LEP individual's bilingual friends or family members, particularly children, is generally not recommended, and departmental personnel shall make case-by-case determinations on the appropriateness of using such individuals.
5. If further assistance is needed, the officer will contact communications to locate an interpreter or contact the telephone interpretation services.

##### **B. Field Enforcement and Investigations**

1. Field enforcement will generally include such contacts as traffic stops, pedestrian stops, serving warrants and restraining orders, crowd/traffic control, and other routine field contacts that may involve LEP individuals. The scope and nature of these activities and contacts will inevitably vary. Department personnel must assess each situation to determine the need and availability for translation services to all involved LEP individuals and utilize the methods outlined in this policy to provide appropriate language assistance.

2. Although not every situation can be addressed in this policy, it is important that department personnel are able to effectively communicate the reason for a contact, the need for information, and the meaning or consequences of any enforcement action taken with an LEP individual. It would, for example, be meaningless for an officer to request consent to search if he/she is unable to effectively communicate with an LEP individual.

#### C. Investigative Interviews

1. In any situation where the translation of an interview may contain information that might be used in a criminal trial, it is important to take steps to improve the chances of admissibility. This includes interviews conducted during an investigation with victims, witnesses, and suspects. In such situations, audio recordings of the interviews should be made. Identifying the contact information for the interpreter (e.g., name, address) should be documented in the case report, so the person can be subpoenaed for trial if necessary.
2. Any person selected as an interpreter and/or translator must (1) have demonstrated competence in both English and the non-English language involved, (2) have knowledge of the functions of an interpreter that allow for correct and effective translation, and (3) not be a person with an interest in the case.
3. The person providing interpretation or translation services may be required to establish the accuracy and trustworthiness of the interpretation or translation to the court.

#### D. Custodial Interrogations and Booking

1. To ensure that the rights of LEP individuals are protected this department places a high priority on providing competent interpretation during arrests and custodial interrogations. It is further recognized that miscommunication during custodial interrogations may have a substantial impact on the evidence presented in any related criminal prosecution. Toward this end, department personnel providing interpretation services or translated forms in these situations will have demonstrated competency in interpretation/translation services and make every reasonable effort to accurately interpret/translate all communications with LEP individuals.
2. If time and opportunity exist, the prosecutor's office should be consulted regarding the proper use of an interpreter prior to any interrogation.
3. To ensure that translations during criminal investigations are documented accurately and that they are admissible as evidence, interviews with victims and all interrogations should be recorded.

4. Employees providing interpretation or translation services shall also be aware of the inherent communication impediments to gathering information from the LEP individual throughout the booking process or any other situation in which a LEP individual is within the control of department personnel. It is important for members of this department to make every reasonable effort to provide effective language services in these situations. Medical screening questions are commonly used to elicit information on an individual's medical needs, suicidal inclinations, presence of contagious diseases, potential illness, symptoms that manifest themselves upon withdrawal from certain medications, or the need to segregate the arrestee from other prisoners.

#### E. LEP Contacts and Reporting

When interpretation or translation services are provided to any involved LEP individual such services should be noted in the related report or any other required documentation.

### V. DEPARTMENTAL RESPONSE FOR LEP

- A. Since there are potentially hundreds of languages department personnel could encounter, the department will utilize the four-factor analysis outlined by the Department of Justice in determining which measures will provide reasonable and meaningful access to various rights, obligations, services, and programs to individuals within this jurisdiction. It is recognized that law enforcement contacts and circumstances will vary considerably. This analysis, therefore, must remain flexible and requires an ongoing balance of the following four factors:
  1. The number or proportion of LEP individuals eligible to be served or likely to be encountered by department personnel or who may benefit from programs or services within the department's jurisdiction or a geographic area.
  2. The frequency with which LEP individuals are likely to encounter department personnel, programs, or services.
  3. The nature and importance of the contact, program, information, or service provided.
  4. The cost of providing LEP assistance and the resources available.
- B. As indicated above, the intent of this analysis is to provide a balance that reasonably ensures meaningful access by LEP individuals to critical services while not imposing undue burdens on the department or on department personnel.
- C. While this department will not discriminate against or deny any individual access to services, rights, or programs based upon national origin or any other protected interest or right, the above analysis will be utilized to determine the availability and level of assistance provided to any LEP individual or group.



#### D. Types of LEP Assistance.

1. Department-provided assistance. Depending on the balance of the four factors listed in A above, this department will make every reasonable effort to provide meaningful and timely assistance to LEP individuals through a variety of services, where available. Department-provided interpreter services may include, but are not limited to, the assistance methods described in this section.
2. Non-departmental assistance. LEP individuals may elect to accept interpreter services offered by the department at no cost, or they may choose to provide their own interpreter services at their own expense. Department personnel should document in any related report whether the LEP individual elected to use interpreter services provided by the department or decided to use a resource of his/her own choosing.
3. Non-certified employee interpreters. Employees utilized for LEP services need not be certified as interpreters, but must have demonstrated, through established department procedures, a level of competence to ascertain whether the employee's language skills are best suited to monolingual (direct) communications, interpretation, translation or all or none of these functions.
4. Out-of-department assistance. When bilingual employees of this department are not available, employees from other city departments who have the requisite training may be requested.

#### E. Written Forms and Guidelines

This department will determine the most frequently used and critical forms and guidelines and translate these documents into the languages most likely to be requested. The department will arrange to make these translated forms available to departmental personnel and other appropriate individuals.

#### F. Telephone Interpreter Services

The administrative section will maintain a list of qualified interpreter services which, upon approval of a supervisor, can be contacted to assist LEP individuals. Such services shall be available to, among others, department personnel who have access to official cellular telephones.

## G. Community Volunteers and other Interpretive Sources

Where competent bilingual departmental personnel or other certified staff are unavailable to assist, responsible members of the community who have demonstrated competence in either monolingual (direct) communication and/or in interpretation and translation may be called upon to assist in communication efforts. Sources for these individuals may include neighboring police departments, university/college languages and linguistics departments, local businesses, banks, churches, neighborhood leaders, and school officials. NOTE: If these outside resources are used, department personnel should ensure that these community members are able to provide unbiased assistance and properly document in any required reports.

## H. Complaints

The department shall ensure access to LEP persons who wish to file a complaint regarding the discharge of departmental duties. The department may do so by providing interpretation assistance or translated forms to such individuals. The department's response to complaints filed by LEP individuals will be communicated in an accessible manner.

## I. Community Outreach

Community outreach programs and other such services offered by this department have become increasingly recognized as important to the ultimate success of more traditional law-enforcement duties. This department will continue to work with community groups, local businesses, and neighborhoods to provide equal access to such programs and services to LEP individuals and groups.

## J. Training

In an effort to ensure that all employees in public-contact positions or employees having contact with those in custody are properly trained, the department will provide periodic training to personnel about departmental LEP policies and procedures, including how to access department authorized, telephonic, and in- person interpreters and other available resources.

## K. Interpreters and Translators

1. Training: Employees called upon to interpret, translate, or provide other language assistance will be trained on language skills, competency (including specialized terminology), and ethical considerations.
2. Assessment: Department personnel identified as bilingual who are willing to act as authorized interpreters will have their language skills assessed by a professional interpreter using a structured assessment tool. Those employees found proficient in interpreting into and from the target language will be placed on the authorized-interpreters list.

3. Reassessment for Authorized Interpreters: Those persons who have been placed on the authorized interpreter list must be re-assessed periodically
4. Additional or refresher language training will be provided by the department periodically.
5. Employees will be responsible for maintaining their proficiency and having their training and assessment results maintained in the training record.
6. The administration section will ensure that the authorized-interpreters list is kept current and a copy of the current list is maintained in the communications center.


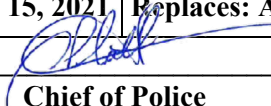
#### L. Supplemental Materials Provided

The following materials will be made available to employees to assist in providing access and service to LEP individuals:

1. Listing of departmental bilingual employees, languages spoken, contact, and shift information.
2. Listing of department certified interpretation services bilingual interpreters, languages spoken, contact, and availability information.
3. Phone number and access code of telephonic interpretation services.
4. Language identification card.
5. Translated Miranda-warning cards and other frequently used documents.
6. Any audio recordings/warnings that are developed in non-English languages.

#### M. LEP Coordinator

1. The Chief of Police will appoint a department supervisor as LEP coordinator who is to be responsible for coordinating and implementing all aspects of the LEP services.
2. Using the four- factor analysis, the LEP coordinator shall assess demographic data, review contracted language access services utilization data, and consult with community-based organizations annually in order to determine if there are additional languages into which vital documents should be translated.
3. The LEP coordinator will also be responsible for annually reviewing all new documents issued by the department to assess whether they should be translated.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.6 Communication with the Deaf or Hard of Hearing</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b>	

**I. POLICY**

It is the policy of this agency to ensure that a consistently high level of service is provided to all community members, including those who are deaf or hard of hearing. This agency has specific legal obligations under the Americans with Disabilities Act and the Rehabilitation Act. To carry out these policies and legal obligations, and to continue to provide the highest level of services to all members of the community, officers will use every means at their disposal to ensure appropriate understanding by those who are deaf or hard of hearing.

**II. PURPOSE**

It is the purpose of this policy to outline the management of communication with individuals who are deaf or hard of hearing.

**III. GENERAL PRINCIPLES**

- A. People who identify themselves as deaf or hard of hearing are entitled to a level of service equivalent to that provided hearing persons.
- B. The agency will make every effort to ensure that its officers and employees communicate effectively with people who are deaf or hard of hearing.
- C. Effective communication with a person who is deaf or hard of hearing who is involved in an incident -- whether as a victim, witness, suspect, or arrestee -- is essential in ascertaining what occurred, the urgency of the matter, and type of situation.

**IV. PROCEDURES**

Communication problems in police-public encounters provide the basis for potential frustration and embarrassment. Failure of officers to recognize that a person has a hearing impairment, or that person’s failure to make his or her impairment known to officers, can also lead to critical misunderstandings. To avoid such potentialities, officers shall be cognizant of the following:

- A. Be alert to indications that a person may be deaf or hard of hearing. Such indications include but are not limited to the following:

1. The appearance of bumper stickers, rear window decals, or visor notices/symbols indicating the disability.
  2. Use of signs, hand signals, or gestures used in attempting to communicate.
  3. Display of cards by the person noting his or her hearing disability.
  4. Inability or difficulty of a person to follow verbal instructions or to reply to requests for information.
  5. A need to see the officer's face directly, suggesting that the person is attempting to lip-read.
  6. Evidence of assistive devices such as hearing aids, cochlear implants, or picture symbols.
  7. Evidence of behaviors such as increased agitation or irritability, low frustration levels, withdrawal, poor attention, or impaired equilibrium.
- B. When interacting with persons who are, or who are suspected of being, deaf or hard of hearing, officers shall never assume that the person understands until it can be confirmed by appropriate responses to questions or directives.
- C. Once someone is identified as deaf or hearing impaired, officers shall determine by written or other forms of communication the person's preferred means of communication—sign language, reading and note writing, lip reading, or speech.
- D. For persons who use sign language, a family member or friend may interpret (1) under emergency conditions or (2) in minor situations and for the sake of convenience, when an interpreter is not available or required by law. In all other situations, officers shall not rely on family members or friends for sign-language interpretation due to their potential emotional involvement or conflict of interest.
- E. Officers shall test comprehension by seeking appropriate responses to simple questions or directives.
- F. Officers must realize that deaf or hard-of-hearing persons may require more time to understand and respond to commands, instructions, and questions than those who hear well.

## **V. COMMUNICATION AIDS**

Various types of communication aids --- known as "auxiliary aids and services" --- are used to communicate with people who are deaf or hard of hearing. These include use of gestures or visual aids to supplement oral communication, an exchange of written notes, use of a computer or typewriter, use of assistive listening devices (to amplify sound for persons who are hard of hearing), and use of qualified oral or sign-language interpreters.

- A. The type of aid that will be required for effective communication will depend on the individual's usual method of communication, and the nature, importance, and duration of the communication at issue. The more lengthy, complex, and important the communication, the more likely it is that a qualified interpreter will be required for effective communication with a person whose primary means of communication is sign language or speech reading. For example:
  - 1. If there has been an incident and the officer is conducting witness interviews, a qualified sign language interpreter may be required to communicate effectively with someone whose primary means of communication is sign language.
  - 2. If a person is asking an officer for directions to a location, gestures and an exchange of written notes will likely be enough to communicate effectively, a sign language interpreter is often not required.
- B. To serve everyone effectively, primary consideration should be given to the communication aid or service that works best for that person. Officers must ask persons who are deaf or hard-of-hearing what type of auxiliary aid or service they need. Officers must defer to those expressed choices, unless there is another equally effective way of communicating, given the circumstances, length, complexity, and importance of the communication, as well as the communication skills of the person who is deaf or hard of hearing.
- C. The agency is not required to provide an auxiliary aid or service if doing so would fundamentally alter the nature of the law-enforcement activity in question, or if it would cause an undue administrative or financial burden. Only the Chief or his or her designee may make this determination.
- D. The input of people who are deaf or hard of hearing who are involved in incidents is just as important to the law-enforcement process as the input of others. Officers must not draw conclusions about incidents unless they fully understand -- and are understood by -- all those involved, including persons who are deaf or hard of hearing.
- E. People who are deaf or hard of hearing must never be charged for the cost of an auxiliary aid or service needed for effective communication.

## **VI. ON-CALL INTERPRETIVE SERVICES**

- A. The agency will employ efforts to maintain a list of sign language and oral interpreting services that are available (on-call 24 hours per day) and willing to provide qualified interpreters as needed. Each of these services will be chosen after having been screened for the quality and skill of its interpreters, its reliability, and other factors such as cost. The agency will update this list annually.
- B. A qualified sign-language or oral interpreter has the following characteristic:
  - 1. Must be able to interpret effectively, accurately, and impartially, both receptively and expressively, using any necessary specialized vocabulary.

2. Must be able to interpret in the language the deaf person uses (e.g., American Sign Language or Signed English) and must be familiar with law-enforcement terms and phrases.

NOTE: Certification is not required for an interpreter to be “qualified.” For example, a certified interpreter who is skilled in American Sign Language would not be qualified to interpret for a person who uses Signed English. Some who are certified might not be familiar with law-enforcement terms or phrases.

- C. In cases where a deaf or hard-of-hearing individual may be charged with a serious crime, the District Attorney should be consulted for appropriate determination of the interpretive services required prior to any interview or interrogation.

## **VII. ARREST SITUATIONS**

- A. Recognizing that some persons need their hands free to communicate, officer should not use handcuffs unless it is necessary for the safety of officers or others. If handcuffs are required, all essential communication with the suspect should be completed prior to their application if possible.
- B. Deaf persons and persons who have severe hearing impairments often have poor verbal communication skills. Their speech may be incoherent or otherwise resemble that of an individual who is intoxicated. They may have difficulty with equilibrium. Officers shall avoid administering standard field sobriety tests to such persons. Breathalyzer, blood alcohol, or horizontal gaze nystagmus should be employed as alternative tests.
- C. Some deaf and hearing-impaired persons have limited written language skills, particularly involving difficult matters such as legal warnings and admonitions. Therefore, officers shall not assume the effectiveness of this form of communication and should gain confirmation of a person’s understanding whenever possible.
- D. Officers shall ensure that deaf and hearing-impaired persons who are arrested and transported to a booking site have their communication devices with them.


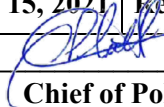
## **VIII. TECHNIQUES FOR OFFICERS TO COMMUNICATE EFFECTIVELY**

Officers must review and have a working knowledge of “Guide for Law Enforcement Officers When In Contact With People Who Are Deaf or Hard of Hearing” [Found in Appendix A of this policy manual] This document reviews how officers should communicate effectively in situations that officers frequently encounter. These situations include the following:

- A. Issuing a non-criminal or motor vehicle citation.
- B. Communicating with a person who initiates contact with an officer.
- C. Interviewing a victim or a witness to an incident.
- D. Questioning a person who is suspected of committing a crime.

- E. Making an arrest or taking a person into custody.
- F. Issuing Miranda warnings to a person under arrest or in custody.
- G. Interrogating a person under arrest or in custody.



	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 7.7 Arrests of Transgender, Intersex, Gender Nonconforming (TIGN) Individuals</b>
	Effective Date: <b>November 15, 2021</b>   Replaces: <b>All Previous Versions</b>
	Approved: _____ <div style="text-align: center;">   <b>Chief of Police</b> </div>
	Reference:

## I. POLICY

It is the policy of this department to recognize the rights of all persons and to treat all persons with the dignity and respect due every individual as a human being. Personnel will act, speak, and conduct themselves in a professional manner, recognizing our obligation to safeguard life and property and to maintain a courteous, professional attitude in all contacts with the public. Personnel will not exhibit any bias or prejudice and they will not discriminate against an individual or group of Transgender, Intersex, and Gender Nonconforming (TIGN) individuals. Department personnel shall take all necessary precautions to ensure the safety of TIGN individuals who are arrested and detained.

Inappropriate or disrespectful interactions with TIGN individuals can interfere with the ability to provide police assistance. A pattern of this kind of conduct can generate a climate of fear or apprehension in which TIGN individuals are afraid or are too uncomfortable to report crime, limiting the department in its ability to provide a safe community.

## II. PURPOSE

The purpose of this policy is to establish standards for interactions with transgender, intersex, and gender nonconforming (TIGN) individuals which provides safety and respect for all persons. It also defines certain terms that pertain to processing TIGN individuals and establishes procedures for processing and holding TIGN arrestees.

## III. DEFINITIONS

- A. Gender Identity or Expression: The actual or perceived identity or behavior of a person as being male or female.
- B. Transgender: Refers to any person whose gender identity or expression differs from the one which corresponds to the person's sex at birth. This term includes transsexuals, intersex individuals, and those whose identity is perceived to be gender nonconforming.
- C. Transsexual: A person whose personal sense of their gender conflicts with their anatomical sex at birth.

- D. Sexual Orientation: An individual's enduring romantic, emotional, and/or sexual attraction to individuals of a specific gender.
- E. Intersex: an individual displaying sexual characteristics of both male and female.
- F. Cross-Dresser: A term that refers to individuals whose clothing is typically associated with the clothing of the opposite sex.

#### **IV. PROCEDURES**

##### **A. Determining Transgender Status**

1. Officers shall follow the below procedures governing interactions with transgender persons when either of these conditions are met:
  - a. An individual explicitly informs an officer that he/she is a transgender person.
  - b. An officer has good reason to believe that the individual is a transgender. Good reason may be based on apparent intention of gender appearance and presentation, reasonable observation, frisking that inadvertently discloses transgender status, background checks, third-party information, and routine policing procedures.
2. When an individual self-identifies as a transgender person, officers shall not question this identity or ask about the person's surgical status except for compelling and professional reasons that can be clearly articulated.

##### **B. When contacting a TIGN individual, personnel will do the following:**

1. Respectfully treat TIGN individuals in a manner appropriate to the individual's gender expression.
2. Use pronouns as requested by a TIGN individual. Use "she," "her," "hers" for a person who self-identifies as a female. Use "he," "him," "his" for an individual who self-identifies as a male.
3. When requested, address the TIGN individual by a name based on their gender rather than that which is on their government-issued identification.
4. If a custodial arrest is made, conduct field searches as prescribed in Department Policy 7.4 Searches Incident to Arrest.
5. If a custodial arrest is made, and the individual has had gender change operative procedures and considers himself/herself a gender different than at birth, personnel should check for warrants under both genders.

- C. When contacting a TIGN individual, personnel will not do the following:
1. Stop, detain, frisk, or search any person for the purpose of determining that person's gender or to call attention to the person's gender expression.
  2. Use language that a reasonable person would consider demeaning or derogatory, specifically language aimed at a person's actual or perceived gender identity or expression or sexual orientation.
  3. Consider a person's gender identification as reasonable suspicion or prima facie evidence that the individual is or has engaged in a crime.
  4. Consider the possession of condoms as evidence or intent of criminal activity.
  5. Disclose an individual's TIGN identity to other arrestees, the public, or non-department individuals absent a proper law-enforcement purpose.
- D. Responders to domestic-violence situations shall respond to transgender individuals in a manner that is appropriate to their gender identity. When responding to a domestic violence call, officers will not automatically determine the batterer and survivor based on actual or perceived gender identity and/or sexual orientation but rather on an assessment of the situation.

## **V. GENDER CLASSIFICATION OF TIGN ARRESTEES**

- A. For purposes of departmental records and operations, an arrestee's gender will be classified as it appears on the individual's government-issued identification card.
- B. Arrestees who are post-operative gender re-assigned are the exception to the government-issued identification card.
1. Male-to-female will be processed as female.
  2. Female-to-male will be processed as male.
- C. If a government-issued identification is unavailable, the arrestee will be classified by their genitalia (e.g., Male genitalia will be male and Female genitalia will be female).
- D. In the event a TIGN individual objects to any questioning regarding this sexual classification, the officer should explain the need for searching prior to transport, and the officer should attempt not to unduly embarrass the individual by using an inappropriate search method or jeopardize the individual's safety by inappropriate placement in the holding facility.
- E. In the event there is uncertainty regarding the appropriate classification of an arrestee's gender, a supervisor will be consulted for further guidance on the appropriate classification.

## **VI. SEARCHING AND TRANSPORT OF TIGN INDIVIDUALS**

### **A. Searches of TIGN individuals:**


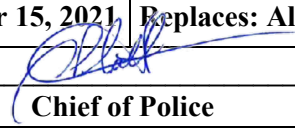
1. Field searches will be conducted by a member who is the same gender as the arrestee based on the gender guidelines as prescribed in Section V of this policy and in accordance with established department search procedures.
2. Personnel taking a TIGN individual into custody, accepting custody from another, or conducting a custodial search will be responsible for conducting a thorough search in accordance with established department procedures.
3. If or when requested by a TIGN individual, department personnel of the TIGN individual's gender identity or expression will be present to observe the custodial search. When practical, the observing member will be a sworn supervisor.
4. Personnel will not conduct more frequent or more invasive searches of TIGN individuals than other individuals.
5. Requests to remove identity-related items -- such as prosthetics, clothing, wigs, and cosmetic items -- will be consistent with requirements for the removal of similar items from non-TIGN arrestees.
6. The possession of a needle that is purported to be for hormonal use will not be presumed to be evidence of criminal misconduct, specifically if the person or arrestee has documentation from a physician for being in the process of a sex modification.

### **B. Transporting TIGN Individuals:**

1. Whenever practical, TIGN arrestees will be transported alone.
2. When requested by a TIGN individual, department personnel of the TIGN individual's gender identity or expression, if available, will be present during the transport.
3. In situations with multiple TIGN arrestees, mass arrests, where a TIGN individual's gender identity or expression is unavailable, or where individual transport is not practical, TIGN arrestees will be transported by gender classification.

## **VII. HOUSING OF TIGN ARRESTEES**

In all cases where a TIGN arrestee is turned over to any other authority for processing or holding it is the officer's responsibility to ensure the receiving officer is made aware of the arrestee's status.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.8 Citizen or Media Recording of Police Activity</b>	
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>	
	<b>Approved:</b>	 <b>Chief of Police</b>
	<b>Reference:</b>	

## I. POLICY

It is the policy of this department that the seizure and searching of portable video, audio, and photo recording devices shall be governed by federal constitutional and statutory laws as well as departmental investigatory policies.

## II. PURPOSE

The purpose of this policy is to establish guidelines and procedures for investigation, seizure, and searching of portable video, audio, and photo recording devices that contain data of an evidentiary value pertaining to a criminal act.

## III. PROCEDURES

### A. General

1. The department recognizes that the taking of photographs and/or videos by private citizens and media personnel is permitted within areas open to general and is protected by the First Amendment.
2. Any civilian or media personnel may video record or photograph a police employee's activities if he/she abides by the following guidelines:
  - a. Remains at a distance that does not physically interfere with the officers' duties.
  - b. Does not physically interfere with the duties and responsibilities of law-enforcement personnel.
  - c. Does not violate any existing statute while taping, e.g. stand in the roadway while filming.
3. Employees are prohibited from arbitrarily seizing a person's portable video, audio, and/or photo-recording without articulable facts to legally justify such a seizure.

B. Initial Contact of an Individual Non-Media Photographer or Videographer: Officers are reminded that there are only three types of encounters between civilians and officers: consensual encounters, temporary detentions based upon reasonable suspicion of criminal activity and an arrest based upon probable cause. It is not a crime to video record or photograph the police. A sworn employee may only contact a person recording images pursuant to these established rules of contact. Sworn employees shall follow the guidelines below:

1. Determine if the encounter is to be consensual in nature, or a lawful seizure.
2. Announce his/her authority and identity.
3. Plain clothes sworn employees shall identify themselves by prominently displaying departmental credentials.
4. Advise the individual of the purpose of the contact.
5. Ask the individual whether he/she recorded/captured data relevant to the incident.
6. Request that the individual provide his or her personal identification and contact information as a witness to the incident.
7. The encounter can last no longer than necessary to effect its purpose.
8. Persons who have been detained, as witnesses or suspects, or those who are participating in a consensual encounter, do not have to give their names, produce identification, or answer questions.

C. Consent to Search and/or Seize Portable Video, Audio, and/or Photo Recording Devices belonging to an Individual (Non-Media Photographer/Videographer)

1. Sworn employees may ask an individual for consent to a search and/or seize a portable photo and/or video recording device to determine if data of evidentiary value pertaining to a criminal act is present.
2. The employee's supervisor shall be notified immediately after any seizure and prior to any search of the device. The supervisor shall determine whether an immediate search is warranted or if there are alternative solutions to the situation.
3. If a consensual seizure occurs, the property shall be inventoried and documented by the seizing sworn employee in accordance with established departmental policy.
4. Authorization to search the device shall be documented by the seizing sworn employee on a consent-to-search form, before beginning the search, and/or video recorded.

5. The seizing sworn employee shall accurately and completely document the basis for the seizure and findings of the search in a case report/offense incident report.

D. Non-consensual Seizure of Portable Video, Audio, and Photo Recording Devices of an Individual (Non-Media Photographer/Videographer)

1. When there is probable cause to believe that the portable video and/or photo recording device depicts visual and/or audio items pertaining to a criminal act, the device may be seized without consent if exigent circumstances exist.
2. The most common type of exigent circumstance is the imminent destruction of evidence. Two requirements must be met for this exigency to exist:
  - a. Sworn employees must have probable cause to believe that evidence that can be destroyed exists.
  - b. Sworn employees must have reason to believe the evidence might be destroyed if they delay acting until a subpoena/search warrant is issued.
3. The sworn employee's supervisor shall be notified immediately after any seizure, and the supervisor shall respond to the scene.
4. No search of the device shall be conducted until a subpoena/search warrant is issued unless there is reason to believe that the immediate search of such materials is necessary to prevent the death of, or serious bodily injury to, a human being.
5. The sworn employee, with guidance of the supervisor, shall be responsible for preparation of an application for subpoena/search warrant.
6. A sworn employee's response to an individual's resistance to a non-consensual seizure shall be to follow department policy.
7. The seizing sworn employee shall accurately and completely document the basis for the seizure in a case report/offense incident report.
8. If a non-consensual seizure occurs, the property shall be inventoried and documented by the seizing sworn employee in accordance with established department policy.

E. Initial Stop of Media Personnel

1. A sworn employee who stops a media photographer/videographer believed to have recorded/captured data of evidentiary value pertaining to a criminal act shall do the following:
  - a. Announce his/her authority and identity

- b. Non-uniform sworn employees shall identify themselves by prominently displaying departmental credentials
- c. Advise the media person of the purpose of the stop
- d. Ask the media person whether he/she recorded/captured data relevant to the incident
- e. If the media person acknowledges recording/capturing relevant data and agrees to allow review and/or supply a copy to the department, the sworn employee shall do the following:
  - i. Immediately notify his/her supervisor
  - ii. Collect and document receipt of the data in accordance with established department policy.
  - iii. Document the request and response on a case report/offense incident report.
- f. If the media person acknowledges recording/capturing relevant data and refuses to allow review and/or provide a copy of the recorded/captured relevant data, or refuses to state whether he/she recorded/captured relevant data, the sworn employee shall do the following:
  - i. Immediately notify his supervisor
  - ii. Instruct the media person not to destroy, alter, or delete the recorded/captured relevant data
  - iii. Document the request and refusal on a case report/offense incident report
  - iv. Assist the supervisor in preparing the appropriate subpoena and/or search warrant documents for production of the requested data
  - v. Request that the media person provide their personal identification, media credentials, and contact information.
- g. The stop shall last no longer than necessary to effect its purpose.

**NOTE:** Brevity is important in determining whether a stop is reasonable. A prolonged stop may be warranted if the employee reasonably and diligently pursues investigative means to determine whether the media person possesses data that may have evidentiary value, and to confirm the person's identity.



2. Sworn employees shall not seize portable video, audio, and/or photo recording devices from media personnel unless they are under arrest or otherwise directly involved in the criminal act.
3. A warrantless search of portable video and/or photo recording devices seized incident to the direct involvement or arrest of media personnel is prohibited unless there is reason to believe that the immediate search of such materials is necessary to prevent the death of, or serious bodily injury to, a human being.

#### F. Supervisory Notification

1. The employee's supervisor shall be notified immediately after the seizure of a portable video, audio and/or recording device, whether consensual or non-consensual, and advised of the following:
  - a. The totality of the circumstances surrounding the stop and seizure
  - b. The type of device seized
  - c. The status of the person from whom the device was seized (e.g. detained, arrested, etc.).

#### G. Supervisor's Responsibilities

1. The supervisor shall do the following:
  - a. Immediately respond to the scene
  - b. Ensure that the circumstances surrounding the seizure as conveyed by the sworn employee are serious enough to warrant the seizure, and that the actions of the officer are following this general order and the department's SOP.
  - c. If the supervisor determines that the stop and seizure is appropriate, he/she shall determine whether a search warrant is appropriate.
  - d. If the supervisor determines that the seizure is not appropriate, he/she will ensure that the portable video and/or photo recording device is immediately returned, and the person detained is made whole.
  - e. The supervisor shall document these findings in a case supplemental report/supplemental report.
  - f. Ensure that the seizing sworn employee documents the circumstances and actions taken in a case report/offense incident report.
  - g. Ensure that all required documentation is completed.

- h. Ensure that proper evidence handling protocols are followed.
- i. Ensure that the Chief of Police has been notified.
- j. Ensure that a use of force report is completed if necessary.
- k. Ensure that any questions or concerns regarding the appropriateness of the stop and/or seizure shall be immediately directed to the next supervisory level in the chain-of-command.
- l. Ensure that the public information office is notified if the supervisor believes that is necessary.

#### H. Impounding of Property

A sworn employee who impounds any portable video, audio, or photo recording device shall follow department policy regarding property/evidence.


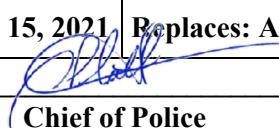
#### I. Prohibited Actions

1. Employees shall not order or participate in the destruction of any portable video, audio, or photo recording devices.
2. Employees shall not order or participate in the erasure, deletion, or destruction of digital, analog, or film evidence.
3. Employees shall not impede a person's right to photograph or video record an event unless that person's actions will have any of the following effects:
  - a. Endangering the safety of the public, employees, or property
  - b. Interfering with an active crime scene
  - c. Violate an existing statute

#### J. Statutory Limitations and Liability

1. Pursuant to federal statute, 42 USC Section 2000aa-6, it is unlawful for a sworn officer or employee, in connection with an investigation or prosecution of a criminal offense, to search for or seize the work product of a media photographer or videographer except in the following circumstances:
  - a. There is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being.
  - b. There is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate.

2. A search or seizure of the work product is prohibited when the offense is merely the withholding of such material.
3. Sworn officers and employees may be held personally liable in an action for civil damages for violation of federal statute, 42 USC Section 2000aa-6.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.10 Prisoner Restraints</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 10.01e</b>	

## I. POLICY

The officer's responsibility for the safe custody of prisoners permits some discretion in the use of handcuffs and other restraining devices. The department requires officers to observe their own safety and that of the people they transport by carefully utilizing restraints on prisoners (except children) who must be taken to a jail or some other location. See also Policy 7.11, Transporting Prisoners.

## II. PURPOSE

The purpose of this policy is to establish guidelines for the use of handcuffs and other restraining devices.

## III. PROCEDURES - Arrested Persons

### A. General

1. Officers shall handcuff all arrested adults unless the application of handcuffs will aggravate or cause injury due to age, infirmity, physical condition, or prior injury.
2. Officers must be able to justify any exception they make to the policy that all arrested adults must be handcuffed, with attention to safety issues.
3. A prisoner who is not handcuffed shall be transported in a vehicle with a prisoner cage, and two officers shall conduct the transport.
4. Juveniles should not be handcuffed unless they have been taken into custody for a violent offense, pose an escape risk, or where the officer reasonably believes handcuffing is necessary for the safety of the juvenile or the officer.

### B. Handcuffs

1. In most circumstances safety concerns mandate that arrested subjects should be handcuffed. Officers must be able to justify exceptions with attention to the risks involved when no handcuffs are used. Listed below are some possible exceptions:

- a. Children under 10 years of age
  - b. Pregnant females
  - c. Handicapped or disabled suspects
  - d. Elderly suspects
2. Normally, officers shall handcuff a subject with the hands in back, but they may choose to handcuff hands in front if the suspect is handicapped or disabled. If the suspect is handcuffed in front, officers should secure the handcuffs to the body by use of a belt if possible.
  3. Officers shall double lock the handcuffs. This will help ensure prisoner and officer safety. Double locking reduces the chance of having the lock picked or that the handcuff will accidentally tighten, which could restrict circulation.
  4. Officers shall apply the handcuffs without utilizing hard strikes to the wrist and no over tightening of the handcuffs.
  5. Individuals will not be handcuffed to any portion of a police vehicle during transport.
- C. Body Belt: The body belt allows the officer to handcuff the prisoner in front while still restricting the movement of the prisoner's arms and hands. The body belt will be used when the officer deems it appropriate.
- D. Ankle Shackles: Ankle shackles shall be used by officers when transporting a prisoner, they have reason to believe might be an escape risk, or when circumstances deem it appropriate in accordance with training.
- E. Plastic Handcuffs: Plastic handcuffs shall be used when officers take several prisoners into custody, or when a prisoner requires multiple restraints. Officers must understand that, once applied, plastic handcuffs can be removed only with a knife, scissors, or other cutting instrument.
- F. Hobble Technique
1. The hobble technique refers to the use of a hobble device to secure a prisoner's feet while in transport in a police car. It involves looping a rope or web belt around the prisoner's ankles and then extending the other end of the device onto the door jam and then shutting the door, thus holding the prisoner's feet in place.

2. The hobble device should be applied only to a prisoner's legs when the officer feels that the prisoner poses an imminent threat of physical harm to himself/herself or another with the use of his/her feet or legs, or when the prisoner attempts to damage the inside of the patrol car during transport.
3. Officers utilizing a hobble device should monitor the status of the prisoner while in transport to prevent the prisoner from harming himself/herself, for example, by head strikes against window.


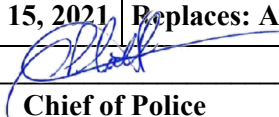
#### **IV. PROCEDURES -- Persons not arrested**

- A. If officers have a reasonable suspicion that an individual has been involved in a violent offense, handcuffs may be applied to such individuals while officers investigate the incident. This restraint is only lawful for safety reasons, and the officers shall articulate the reasons for their safety concern.
- B. Persons not arrested but who are subject to detention may be restrained under the following circumstances:
  1. Suspects shall be handcuffed only if necessary.
  2. Handcuffing of suspects shall be accomplished with minimal discomfort to the suspect.
  4. Officers shall limit the number and type of restraints used on the suspect to what is reasonably necessary.
  5. If an individual is handcuffed or otherwise restrained for officer safety reasons during an investigation and later released, officers shall document their actions in an offense or incident report and include the reasons officers handcuffed the individual, the approximate length of time of the restraint, and the results of the investigation.

#### **V. SPECIAL CIRCUMSTANCES -- Restraint prohibitions**

- A. Officers shall not place subjects in a prone position with the hands and ankles bound behind with handcuffs, belts, or other devices.
- B. As soon as any suspect who is lying on his or her stomach has been handcuffed, officers shall roll the suspect onto his or her side or place the suspect in a sitting position.
- C. Suspects shall never be transported in a prone, face-down position.
- D. All suspects will be monitored during custody and transport for indications of medical problems, and medical treatment will be obtained if the officer believes it is needed or the person in custody requests medical assistance.

E. Officers should be aware that intoxication, recent use of drugs or alcohol, the presence of a head injury, obesity, physical disability, and recent exertion are all circumstances that can increase difficulty breathing when a person is restrained.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.11 Prisoner Transportation</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 10.01, 10.10, and 10.12</b>	

## I. POLICY

Transportation of persons in custody is a constant requirement and a frequent activity. Transportation usually occurs in two instances. The first is immediately after arrest when the arrestee is taken by the arresting officer for booking and holding or transfer to another facility. The second concerns the movement of prisoners from the detention facility for various reasons, such as to the county jail, to a hospital or other medical facility, to court, and for other reasons. Transporting prisoners is a potentially dangerous function. Therefore, it is the policy of this law-enforcement agency to take the precautions necessary while transporting prisoners to protect the lives and safety of officers, the public, and the person in custody.

## II. PURPOSE

The purpose of this policy is to establish procedures to ensure that prisoners are transported safely.

## III. PROCEDURES (Texas Best Practices: 10.01)

### A. General

1. All prisoners shall be transported in secure, caged vehicles, unless such a vehicle is not available.
2. In no case shall a juvenile known or believed to be under the age of 17 years be transported with adults suspected of or charged with criminal acts.
3. When picking up a prisoner from any facility, the officer shall verify the identity of the prisoner.
4. The transporting officer shall obtain from the custodian of the prisoner any paperwork, property, or medical records that should accompany the transfer of the prisoner.



## B. Searching the prisoner

1. The transporting officer shall always search a prisoner before placing him or her into the vehicle. This procedure should be followed regardless if another officer searched the prisoner before the transporting officer took possession of the prisoner.
2. Officers must never assume that a prisoner does not possess a weapon or contraband or that someone else has already searched the prisoner.
3. The transporting officer shall conduct a search of the prisoner each time the prisoner enters custody of the officer.
4. When handling and searching prisoners, officers shall remain mindful of the department's plan for the control of infectious diseases and shall use personal protective equipment when necessary.
5. Any items removed from the prisoner prior to transport will be securely maintained and returned to the prisoner or turned in to the booking officer upon arrival at the location of detention for placement in the prisoner's property. (TEXAS BEST PRACTICES: 10.10)

## C. Searching the police vehicle

The transporting officer shall search the vehicle immediately before each prisoner transport to ensure that no contraband or weapons are available to the prisoner. Further, after delivering the prisoner to his/her destination, officers shall again search the police vehicle to ensure that the prisoner did not hide anything in the vehicle. (TEXAS BEST PRACTICES 10.01)

## D. Transport equipment

1. Most marked vehicles are equipped with a metal or plastic screen to separate the front and rear compartments. Normally, these vehicles will be used in all prisoner transports to prevent prisoner access to the driver's compartment.
2. All vehicles equipped with metal or plastic screen barriers and used in transporting prisoners will have the rear doors child locked or interior door and window handles removed/deactivated in order to minimize the risk of escape by prisoners being transported.
3. At the beginning of each shift and before transporting prisoners, officers shall check their vehicles for proper security measures and any contraband.

## E. Positioning of prisoners in the transport vehicle

1. When an officer transports a prisoner in a caged vehicle, the prisoner shall be positioned in the rear seat and secured with a seat belt. Further, the prisoners shall be handcuffed with their hands behind their backs, palms outward, except for the exceptions detailed in Policy 7.10.

2. When a single officer transports a prisoner in a non-caged vehicle, the prisoner shall be placed in the right front seat and secured with a seat belt. The prisoner shall be handcuffed with his or her hands behind the back, palms outward.
3. A single officer shall never transport two or more suspects in a non-caged vehicle unless directed to do so by the on-duty supervisor.
4. If more than one officer transports prisoners in a non-caged vehicle, the following procedures shall be observed:
  - a. One officer shall sit in the rear of the transporting vehicle behind the driver with the prisoner on the rear passenger side with the seat belt fastened.
  - b. When more than one prisoner is transported by two officers in the same vehicle, the prisoners shall be positioned on the front and rear passenger sides (seat belted) and the assisting officer shall sit behind the driver, in order to protect the driver and be able to monitor the prisoner's actions.
5. Officers shall not transport prisoners who are restrained in a prone position. Doing so increases the risks of medical complications.

F. Control of prisoners while transporting: Observation and Medical Assistance (TEXAS BEST PRACTICES: 10.12)

1. During custody and transportation, officers shall continually observe the prisoner, even when it becomes necessary to allow the prisoner the use of a toilet.
2. If a prisoner appears lethargic, particularly after an active confrontation with officers, or is unresponsive, immediate medical help may be necessary. The officer should observe the suspect carefully and if the officer is in any doubt about the prisoner's health medical assistance shall be summoned immediately.
3. Officers should ask an apparently ill prisoner if he or she wishes medical assistance.
4. The transporting officer shall advise the receiving officer or deputy of any medical conditions of the prisoner, or any suspicions or concerns about the prisoner's physical or mental health.
5. Prisoners shall not be left unattended at any time during transport except for situations in section G. below.

G. Stopping to provide law-enforcement services while transporting

1. When transporting a prisoner, the transporting officer shall provide law-enforcement services only under the circumstances listed below:
  - a. A need exists for the transporting officer to act immediately to stop or prevent a violent act and prevent further harm to a victim.

- b. A person has been injured and assistance is required immediately.
  2. In the above situations, the transporting officer shall ensure the prisoner is secured and protected.
  3. Under no circumstances shall an officer transporting a prisoner engage in a pursuit.
- H. **Escape:** If a prisoner escapes while being transported, the transporting officer shall observe the following procedures:
  1. Request assistance immediately from the jurisdiction the officer is in at the time of the escape.
  2. Provide dispatch with the following information:
    - a. Location of escape.
    - b. Direction and method of travel and means of escape.
    - c. Name and physical description of escapee.
    - d. Possible weapons possessed by the escapee.
    - e. Pending charges.
  3. Try to recapture the escapee as soon as possible.
  4. Submit a written report to the Chief of Police as soon as practical, explaining the circumstances of the escape.
- I. **Prisoner Communication:** The transporting officer shall not allow prisoners to communicate with other people while in transit unless, in the judgment of the officer, the situation requires it.
- J. **Arrival at Destination:** Upon arriving at the destination, the transporting officer shall observe the following procedures:
  1. Firearms shall be secured in a designated place at the facility being entered. If there is no designated place, the firearms shall be locked inside the trunk of the police vehicle away from access to the prisoner.
  2. Restraining devices shall be removed only when the officer is directed to do so by the receiving facility or when the officer is sure that the prisoner is properly controlled and secure.

3. The proper paperwork (booking sheet, arrest report, property form, etc.) shall be submitted to the receiving facility and, in situations that require it, the officer shall ensure that proper signatures are obtained on paperwork to be returned to the department.

K. Sick/injured prisoners and medical facilities


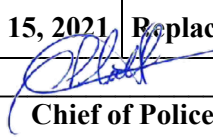
1. Any time -- before, during, or after an arrest -- that the prisoner is injured or becomes sick, the officer shall seek medical attention immediately. Medical attention shall be obtained before transporting the prisoner to the jail if the injury/sickness happens before they arrive at the jail.
2. The transporting officer shall use discretion in the use of restraining devices on sick or injured prisoners.
3. As a rule, do not remove a prisoner's handcuffs at the hospital unless ordered to do so by the attending physician. Violent prisoner's restraints are not to be removed unless the physician has sedated the prisoner to prevent injury to medical staff or the officer.
4. If the prisoner refuses treatment, the prisoner shall be asked to sign a medical-refusal form or notation of such on a hospital release form. The attending physician or a nurse should sign the form as witnesses. If the prisoner refuses to sign the form, the officer should obtain two witnesses to the refusal, for example, a hospital staff member, another officer, or fire/rescue personnel). The form must be given to the jail during booking.
5. If the prisoner must be admitted to the hospital, the officer shall release the prisoner to the hospital only after consulting the on-duty supervisor. The supervisor, in turn, shall consult the magistrate or the city judge.
6. The prisoner shall always be kept under observation and, normally, restraining devices shall be used. Officers shall consult with medical personnel concerning the use of restraining devices.
7. The supervisor shall observe the following procedures to ensure control of the prisoner:
  - a. If the prisoner is admitted and the prisoner was arrested for a felony, arrange for guards.
  - b. Request the presence of a magistrate and arrange for the magistrate's transportation to the hospital so that bail can be set.
  - c. Assist the magistrate in arraigning the prisoner, if necessary, or stand by while the magistrate issues a warrant.
  - d. Serve the warrant if one has been issued.

- e. Arrange for a guard to be maintained until the prisoner makes bond or the case is filed if the magistrate will not release the arrestee on personal recognizance.
- f. When the case is filed, responsibility will transfer to the sheriff's office.
- g. Brief every officer on the duties of guards and ensure that guards have radios.
- h. Ensure that guards are checked periodically and relieved as necessary until sheriff's deputies relieve them.

L. Special transport problems:

- 1. Transport of prisoner by officer of different sex or prisoners that are Transgender, Intersex, and Gender Nonconforming (TIGN) individuals.
  - a. When transporting a prisoner of one sex by an officer of another sex, or TIGN prisoners, the transporting officer shall do the following:
    - i. Contact the dispatcher by radio and request that the time and odometer mileage be logged.
    - ii. Go directly to the destination by using the shortest practical route.
    - iii. Upon arrival at the destination, contact the dispatcher by radio and request that the time and the odometer reading be logged.
- 2. Prisoner with disabilities
  - a. When transporting a prisoner with disabilities, the transporting officer shall request help when needed to complete the transport safely for both the prisoner and the officer.
  - b. The officer may request the dispatcher contact the fire department or ambulance for assistance in transporting.
  - c. The transporting officer shall take whatever special equipment or medicine is necessary for the prisoner.
  - d. With a disabled person in custody, the transporting officer must use common sense. When the disability is such that no danger of escape or injury to the prisoner or officer exists, restraining devices may be inappropriate.
  - e. Any wheelchairs, crutches, and medication shall be transported with, but not in the possession of, the prisoner.

- f. Department personnel have an obligation to provide a “reasonable accommodation” for disabled prisoners. This obligation requires officers to ensure disabled prisoners are not subjected to the possibility of injury or handling of a disrespectful nature during arrest and transportation procedures.
  3. Dangerous/security-risk prisoners. When a prisoner is considered dangerous or a security hazard, the receiving agency’s personnel shall be notified before the transport takes place in order to plan how best to minimize any chance of escape or of injury to the prisoner or anyone else.
- M. Restraining devices: When prisoners are restrained during transport, the following procedures shall be followed unless circumstances require an alternate method:
1. Single prisoner shall be handcuffed with both hands behind his or her back.
  2. Leg and waist belt restraints may also be used to minimize the risk of injury or escape.
  3. Under no circumstances shall a prisoner be handcuffed to a part of the transport vehicle itself, such as the floor post, protective screen barrier, etc.
  4. Officers shall use ankle shackles or plastic handcuffs to immobilize legs when transporting any prisoner that might pose an escape risk.
- N. Documentation:
1. Officers shall document all prisoner transports and shall note any unusual circumstances or events in the arrest report.
  2. Officers shall document the circumstances of any apparently ill or injured prisoners and their medical treatment.
  3. Officers will give names (and badge numbers, as appropriate) of personnel from and to whom the prisoner was released or transferred.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.12 Juvenile Procedures</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 10.02 and 10.03	

## I. POLICY

This department is committed to the development and perpetuation of programs for prevention and control of juvenile delinquency. In dealing with juveniles, officers will use the least coercive methods among available alternatives, consistent with preserving public and officer safety, order, and individual liberty. Among factors to consider in making juvenile dispositions is the nature of the offense; the offender's age, circumstances, and record; availability of rehabilitation programs; and juvenile probation or court recommendation for diversion.

## II. PURPOSE

The purpose of this policy is to establish guidelines and procedures for handling juveniles who need protection, in violation of status offenses, and those charged with criminal offenses.

## III. DEFINITIONS

- A. Child (Juvenile): A person who is ten years of age or older and less than seventeen years of age.
- B. Conduct in Need of Supervision: Conduct: Any offense -- other than a traffic offense -- that violates the penal laws of the state and which are punishable by fine only, violations of municipal ordinances, failure to attend school, and running away.
- C. Delinquent Conduct: Conduct, other than a traffic offense (except DWI), that violates the penal laws of this state or the United States punishable by imprisonment or confinement in jail.
- D. Delinquent child: A child who has committed a delinquent act or an adult who committed a delinquent act prior to his or her 17th birthday.
- E. Intake officer: A juvenile probation officer who is designated by law as having the quasi-judicial authority to decide probable cause, divert the juvenile from the criminal process, or petition the court. An intake officer is normally a juvenile probation officer.

- F. Juvenile court: The court designated under Family Code 51.04 to exercise jurisdiction over juvenile proceedings within the county. As a result, the judge of this court decides the propriety and legality of police handling of juveniles.

NOTE: All juvenile offenses occurring in the City of Teague are heard in Freestone County.

- G. Juvenile processing office: The office or location within the police department or school facility, approved by the juvenile court, for the temporary detention of juveniles while officers complete required activities prior to releasing the juvenile to a parent or transferring the juvenile to the juvenile detention center.

NOTE: The approved Juvenile Processing Office for the Teague Police Department is the Freestone County Juvenile Probation Office, located at 112 E Main St Ste 105, Fairfield, TX 75840. This office will determine the location juveniles are detained, should this be required.

- H. Referral to juvenile court: The referral of a child's case to the official, including the intake officer, designated by the juvenile board to process children within the juvenile justice system.
- I. Responsible or Suitable Adult: In the absence of a juvenile's parents or legal guardian, a responsible adult who is responsible for the physical custody of a juvenile or who is an adult acquaintance of the juvenile's parents or legal guardian who agrees and reasonably demonstrates the ability to provide supervision for the juvenile until parents, legal guardian, or next of kin can assume that responsibility.
- J. Status Offender: A juvenile who is charged with an offense that would not be a crime if committed by an adult, such as violating a curfew or running away.

#### **IV. PROCEDURES – General (TEXAS BEST PRACTICES: 10.02)**

##### **A. Overview**

1. All members of the department shall cooperate with juvenile justice authorities and their support activities.
2. Juveniles have all the same constitutional rights as do adults and all requirements for protection of those rights apply to juveniles as well as adults. Additional rules are prescribed by the Texas Family Code. All department personnel are responsible for following the Family Code and this order. (TEXAS BEST PRACTICES 10.02a)
3. Officers who detain juveniles should first determine if the juvenile is alleged to have been harmed or to be in danger of harm. Those in need of immediate medical treatment will be transported to an appropriate medical facility under the same guidelines as adult prisoners. The Department of Protective and Regulatory Services is to be contacted immediately if there is an indication that the juvenile



cannot safely be released to a suitable adult and the juvenile does not meet criteria for transport to the detention facility.

4. Children under 10 cannot be held responsible through criminal law or the juvenile justice system. If a child under 10 is found in violation, the following applies:
  - a. enforcement action cannot be taken.
  - b. children under 10 cannot be detained at a police facility for criminal violations; however, children may be kept in a non-secure area of a police facility pending arrival of a suitable adult.
  - c. the officer must document the conduct of children under 10 that would ordinarily be a criminal or juvenile code violation if they were classified as a juvenile on the appropriate report form to include any applicable identifiers.

#### B. Handling of Juvenile Offenders - General

1. A juvenile offender shall be handled with firmness and respect.
2. The juvenile justice system and laws are designed to give the child a chance to mature without bearing the stigma of a criminal record.
3. The juvenile justice system emphasizes confidentiality of records and the privacy of an adjudicatory hearing.
4. Where appropriate, officers shall reasonably try to keep juveniles out of the criminal justice system.
5. The taking of a juvenile into custody is not an arrest except for the purpose of determining the validity of taking the juvenile into custody or the validity of a lawful search.
6. All investigative detentions and enforcement actions involving juveniles will be documented, either by use of a written warning, citation, or incident/offense report.
7. All contacts with juveniles will be recorded as best as possible on the in-car audio/video system.

#### C. Authority for Taking a Child into Custody

1. A juvenile may be taken into custody in the circumstances listed in 52.01 of the Family Code, by a Directive to Apprehend as outlined by 52.015 of the Family Code, or with probable cause. Section 52.01 of the Family Code specifies that a child may be taken into custody by a law enforcement officer when a child engages in any of the following:

- a. Conduct that violates a penal law of this state or a penal ordinance of any political subdivision of this state,
  - b. Delinquent conduct or conduct indicating a need for supervision, or
  - c. Conduct that violates a condition of probation imposed by the Juvenile Court
2. Section 52.01 also authorizes officers to release a juvenile with a warning in lieu of custody. If the child is released with a warning it is necessary to forward a copy of the warning to the parent. In making the decision to handle the juvenile either informally with a warning or formally by referral to the juvenile court, the officer shall consider the following:
- a. Seriousness of offenses.
  - b. Prior record of child.
  - c. Child's age.
  - d. Cooperation and attitude of all parties (child, parent, victim) and,
  - e. The possibility of the offense being repeated.
  - f. Degree of wrongful intent, violence, premeditation, knowledge of violation.

#### D. Enforcement Alternatives

1. Officers dealing with juveniles in enforcement capacities may exercise reasonable discretion as outlined in this policy in deciding on appropriate actions. Alternatives that may be considered include the following, listed in order of severity: release without further action, release with verbal warning, referral to parents or responsible adult, or informal counseling with contact of parents or responsible adult.
  - a. field release with written warning or citation, limited custody and station-house warning, arrest under non-secure custody, and release to parents with or without referral to juvenile court or first-offender program; and
  - b. arrest and secure custody, with transfer to detention and referral to juvenile court.
2. Enforcement criteria for the use of these alternatives are provided below.

3. Even when a juvenile is being handled informally, the juvenile has all the constitutional rights that an adult would have in the same situation.
4. In all cases where a juvenile is believed to have committed a violation, regardless of the disposition, officers shall make every reasonable attempt to notify parents or guardians and inform them of the circumstances of the contact.

## **V. ENFORCEMENT CRITERIA**

- A. The following general guidelines may be used in determining appropriate enforcement and related actions that may be taken when dealing with juvenile incidents.
  1. Release without further action, release with verbal warning, and referral to parents or responsible adult, or informal counseling with contact of parents or responsible adult.
    - a. Appropriate incidents where no violation was determined or where the violation was very minor, and officers explained the law and consequences.
      - i. No property damage or personal injury was involved.
      - ii. No prior record exists.
      - iii. May include contact with parent if appropriate.
      - iv. Examples of these incidents include, but are not limited to, curfew violations, minor liquor law violations, and disorderly conduct.
    - b. If a non-traffic citation is issued, the juvenile's parents may be contacted by telephone from the scene and advised of the offense and disposition. If the parents cannot be contacted, officers will make a copy of the citation and forward the copy by mail, to the parents. On it, the officer shall give a complete description of the circumstances of the contact. Parental contact information should be included on the citation, to assist the court in making contact for case disposition.
    - c. If officers detain a juvenile for a non-traffic offense and decide not to issue a warning or citation, officers shall complete an incident report and forward it to the parents by mail or deliver the copy in person.
  2. Field release with written warning or citation, or limited custody and station-house warning, arrest under non-secure custody, and release to parents with or without referral to juvenile court or first-offender program.

- a. Officers may elect to transport the youth home, make personal or telephone contact with the youth's parents or guardians to provide them with information and counseling on their child's actions, or take the youth into custody and transport the youth to the juvenile processing office until he/she is released to a parent or guardian.
    - i. Appropriate when the nature of the incident is of a more serious or potentially serious nature than in section 1 above.
    - ii. There was property damage or minor injury not amounting to a felony.
    - iii. The youth involved is fully aware of the seriousness or potential seriousness of his/her actions and/or is acting in alliance or collusion with others to commit such acts.
    - iv. The youth fails to cooperate or to positively respond to police intervention and direction.
    - v. The youth's parents or responsible adult have apparently failed to provide appropriate control and supervision.
  - b. Officers may elect to file a referral to the juvenile court depending on the nature of the offense and prior history of the offender.
  - c. Officers releasing a juvenile to the custody of their parents shall complete a juvenile release form, which is signed by the parent or legal guardian, to include with their case reports.
3. Arrest and secure custody, with transfer to detention and referral to juvenile court. Officers may file delinquency charges against a juvenile when the circumstances surrounding the incident meet or exceed the seriousness of those cited as examples in section 2 above.
- a. Officers should file delinquency charges against juveniles when they commit any of the following:
    - i. Acts that if committed by an adult would be felonies.
    - ii. Delinquent acts involving deadly weapons.
    - iii. Serious gang-related offenses.
    - iv. Delinquent acts involving serious assault.
    - v. Delinquent acts while on probation or parole or when they have charges pending against them.

- vi. Delinquent acts as repeat offenders or when the juveniles have refused to participate in diversion or intervention programs; or
  - vii. When it has been determined that parental or other adult supervision is ineffective.
4. Status Offenses. Based on the seriousness of and circumstances surrounding the offense, the background and demeanor of the juvenile, and other relevant factors, an officer may release a juvenile to his parents, guardian, or other responsible adult.
- a. Juveniles taken into custody for status offenses should normally be frisked for weapons prior to being transported and may be handcuffed or otherwise restrained at any time if, in the judgment of the officer, the juvenile poses a physical risk to the officer, or others.
  - b. Officers shall pay special attention to juveniles under the influence of alcohol or drugs to determine whether emergency medical services are warranted.
  - c. Juveniles taken into custody for status offenses shall be held in non-secure custody as provided by state law and for the briefest time necessary to conduct identification, investigation, and related processing requirements to facilitate their release to a parent or responsible adult or transfer to a juvenile facility.
  - d. Transportation of a juvenile in a caged vehicle is not considered secure custody.
  - e. Status offenders and other juveniles taken into temporary non-secure custody for status offenses should not be fingerprinted or photographed for purposes of record.
  - f. Status offenders in temporary custody shall not be placed in a holding area with adult suspects and shall also be under constant visual supervision. Status offenders will be afforded reasonable access to toilets and washing facilities; provided food if they are in need of nourishment to include any special diets necessary for health or medical purposes; provided with reasonable access to water or other beverages; and allowed reasonable access to a telephone.

## **VI. JUVENILE PROCESSING**

- A. Searching and Transportation of Juveniles (TEXAS BEST PRACTICES 10.02 b, c, d)
  - 1. No juvenile under 17 shall be transported in the same vehicle with adults suspected of or charged with criminal acts.

2. Juveniles are searched and transported in the same manner as adults in compliance with Policy 7.11 Prisoner Transportation.
3. Juveniles are typically not handcuffed unless they have been taken into custody for a violent offense, pose an escape risk, or where the officer reasonably believes handcuffing is necessary for the safety of the juvenile or officer. The utilization of handcuffs is at the discretion of the officer taking the juvenile into custody. Officers will double lock and check the handcuffs for tightness. Officers will check the handcuffs if there is a complaint that they are too tight.
4. An officer transporting a juvenile should notify the dispatcher that the officer will be transporting a juvenile along with the juvenile's gender. The officer should also notify the dispatcher of the officer's location and mileage on the vehicle upon initiating the transport and the officer's ending mileage and location upon arrival at the officer's destination. The officer should monitor the prisoner during the transport for any medical issues.
5. Recording and video equipment shall be activated during transport.

B. Actions when taking a juvenile into custody

1. A person taking a child into custody shall advise the juvenile of his/her constitutional rights when appropriate.
2. Without unnecessary delay and without first taking the child elsewhere, the officer does one of the following:
  - a. Releases the juvenile to a parent, guardian, custodian, or other responsible adult.
  - b. Brings the juvenile before an official of the juvenile court.
  - c. Takes the juvenile to a detention facility designated by the juvenile court.
  - d. Takes the juvenile to a medical facility if the juvenile is believed to be suffering from a serious physical condition or illness that requires immediate treatment.
  - e. Takes the juvenile to the intoxilyzer room if in custody for an offense requiring a breath specimen, but the juvenile must be taken to one of the above-mentioned locations upon completion of the intoxilyzer test.
  - f. In cases of truancy, immediately takes the juvenile to the proper school official within the appropriate public or private school.
  - g. Takes the juvenile into protective custody if the officer believes the juvenile is in danger of harm; or

h. Releases the child with no further action pending.

C. Notifications:

1. The arresting officer shall promptly notify the juvenile's parents or guardians of the fact that the child has been taken into custody. In the case of protective custody, the notice must be written as prescribed by the Texas family code. Notification of the parents or attempts at notification shall be documented in the arrest report.
2. The arresting officer shall comply with VIII (D) of this policy, if applicable.

D. Designated Juvenile Processing Area: (TEXAS BEST PRACTICES 10.02 e, and 10.03)

1. A juvenile may be detained in a holding area certified by the juvenile court. The Teague Police Department's approved juvenile processing will be posted with the authority letter from the local juvenile authorities.
2. Juveniles are detained under the following conditions:
  - a. At no time is a juvenile placed in a jail cell designated for the holding or incarceration of an adult.
  - b. At no time will a juvenile who is in custody be left unsupervised in the juvenile holding area.
  - c. All juveniles held in the juvenile processing office will be out of sight and sound of adult prisoners.
  - d. No juvenile is held in custody longer than is reasonably necessary to investigate, prepare a case, or to await the arrival of a parent or guardian.
  - e. At no time will a juvenile be held in the juvenile processing office longer than six hours. If not otherwise released, the juvenile will be taken to the juvenile detention facility within six hours of the arrest.

E. Taking a Runaway into Custody

An officer who has probable cause to believe that a juvenile has run away from home shall perform the following:

1. Verify the juvenile's status as a runaway.
2. Take the child into custody.
3. Release the juvenile to a parent, guardian, legal custodian, or other person acting in loco parentis.

4. If a parent or some other responsible party cannot be located, take the juvenile to the juvenile processing office, and contact the juvenile detention center intake officer for instructions.

NOTE: The juvenile processing office may not be locked when holding status offenders, and an officer will remain with the juvenile until disposition is made.

5. Notify Communications to remove the runaway report from the computer system.
6. Complete incident reports for any runways taken into custody.
7. If the child is an out-of-town runaway, take the child into custody and verify runaway status with the other jurisdiction.
8. If a detention order is on file, follow the instructions for serving a detention order.
  - a. Notify the intake officer of the juvenile court of the action taken. The intake officer will then determine what the next step will be. The officer shall:
    - i. Follow the intake officer's instructions for detention or child placement.
    - ii. Notify parents that the child is in custody.
    - iii. If the child is to be released and the parents cannot respond within a reasonable time, then arrange to detain the juvenile.

#### F. Taking a Truant into Custody

1. An officer who takes a juvenile into custody because school officials have reported that the juvenile is a truant shall deliver the juvenile to the school and release him/her to appropriate school personnel.
2. The officer shall complete an incident report that includes the name of the person notifying the parent of the truancy and the name of the person to whom the juvenile was released.

### **VII. PROTECTIVE CUSTODY**

- A. A law-enforcement officer may take protective custody of a child without a court order for the following reasons and no others:
  1. Upon discovery of a child in a situation of danger to the child's physical health or safety when the sole purpose is to deliver the child without unnecessary delay to the parent, managing conservator, possessory conservator, guardian, caretaker, or custodian who is presently entitled to possession of the child.



2. Upon the voluntary delivery of the child to the law-enforcement officer by the parent, managing conservator, guardian, caretaker, or custodian who is entitled to possession of the child.
3. Upon personal knowledge of facts that would lead a person of ordinary prudence and caution to believe that there is an immediate danger to the physical health or safety of the child and that there is no time to obtain a temporary restraining order or writ.
4. Upon information furnished by another which has been corroborated by personal knowledge of facts, all of which taken together would lead a person of ordinary prudence and caution to believe that there is an immediate danger to the physical health or safety of the child and there is no time to obtain a temporary restraining order or writ.
5. Upon personal knowledge of facts that would lead a person of ordinary prudence and caution to believe that the child has been the victim of sexual abuse and that there is no time to obtain a temporary restraining order or writ.
6. Upon information furnished by another that has been corroborated by personal knowledge of facts and all of which taken together would lead a person of ordinary prudence and caution to believe that the child has been the victim of sexual abuse and that there is no time to obtain a temporary restraining order or writ.
7. Emergency Treatment for Juveniles: In the absence of the responsible parent or guardian, police officers are expected to take immediate custody of any juvenile found to need emergency medical care and to see that the juvenile is taken to an emergency hospital for treatment.

#### B. Procedures for Taking Custody of Juvenile in Need of Emergency Treatment

1. When it is found that a juvenile has been injured or is ill to the extent that immediate emergency care is necessary to protect the physical well-being of the juvenile and no responsible parent or guardian can be found, the below listed procedures are followed to obtain the necessary medical care in an expeditious manner:
  - a. The officer either takes custody of the juvenile and delivers him/her to the nearest competent emergency hospital, or the officer requests an ambulance and orders the juvenile taken to the nearest competent emergency hospital.
  - b. The officer utilizes all available resources to immediately contact a parent or guardian (school officials, etc.).
  - c. The officer will immediately notify the Child Protective Services office of the circumstances at hand and furnish the Child Protective Services office the following information:

- i. Name, race, and date of birth of the juvenile.
  - ii. Name and address of parents if available.
  - iii. What hospital the juvenile has been taken to.
  - iv. What efforts have been made to contact the child's parents or guardian.
2. Follow-Up Investigation:
- a. The officer conducts a follow-up investigation at the receiving hospital, being sure to explain the circumstances at hand to the proper hospital representative.
  - b. Supervisors will take over hospital follow-up investigations, if necessary, when it becomes apparent that such investigations will be lengthy or complex.
  - c. Supervisors will follow-up if it becomes apparent that the child's injury is due to criminal conduct on the part of any person.

C. Persons Who May Consent to Medical Treatment:

The Texas Family Code allows any of the following persons to consent to medical, dental, psychological, and/or surgical treatment of a child when the person having the right to consent as otherwise provided by law cannot be contacted and that person has not given actual notice to the contrary:

- 1. A grandparent, adult brother or sister, adult aunt or uncle of the child; an educational institution in which the child is enrolled that has received written authorization to consent from the person; an adult who has actual care, control, and possession of the child and who has written authorization to consent from the person having the right to consent.
- 2. A peace officer who has lawfully taken custody of a minor if the peace officer has reasonable grounds to believe the minor needs immediate medical treatment.
- 3. Any court having jurisdiction over the child.

**VIII. INVESTIGATIVE PROCEDURES**

A. Custodial Interrogation of Juveniles

- 1. Custodial interrogation of juveniles by department employees shall adhere strictly to procedural requirements established by the Texas Family Code and relevant court rulings.

2. The custodial officer interviews the juvenile. The officer explains to the juvenile the procedures that will relate to their case. The officer or detective may, at their discretion, allow other persons to be present during the interview. An attorney representing the child is allowed if requested.
3. The interrogation of a juvenile is completed within a reasonable time or terminated if the juvenile requests the interrogation be terminated.

B. Written Confessions/Statements:

Written confessions from juveniles must be taken in compliance with the Texas Family Code, outlined below.

1. A magistrate, outside the presence of law-enforcement officers, first warns the juvenile.
2. An officer then takes the typed or handwritten confession but leaves the statement unsigned.
3. The officer then returns the juvenile and the statement to the magistrate.
4. The magistrate will review the statement with the juvenile outside the presence of law-enforcement officers.
5. The juvenile is then allowed to sign the statement in the magistrate's presence.
6. Any recording made of a juvenile interview, audio or video, must also be presented to the magistrate for review.

C. Fingerprinting and Photographing Juveniles:

1. Fingerprints and photographs of juveniles are maintained separately from those of adults.
2. Fingerprints and photographs of juveniles are destroyed as directed by the Texas Family Code.
3. Fingerprints are taken to comply with state reporting requirements.
4. All juveniles placed in custody for cases classified as class "B" misdemeanor or higher are fingerprinted and photographed.
5. These records are maintained at the Juvenile Detention Center or Juvenile Probation Office, and in the appropriate State files.

6. If latent fingerprints are found during the investigation of a case and the law enforcement officer has probable cause to believe that they are those of a particular child, unless otherwise prohibited by law, the officer may fingerprint the child regardless of the age or case for the purpose of immediate comparison with the latent fingerprints.
7. If fingerprints of a child are taken for purposes of comparison and the comparison is negative, the fingerprint card and other copies of the fingerprints taken are destroyed immediately. If the comparison is positive and the child is referred to the juvenile court, the fingerprint card and other copies of the fingerprints are filed locally and with the State. If the child is not referred to the court the fingerprints are destroyed immediately.

#### D. Required Notification of Schools


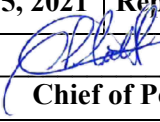
1. An officer who arrests or takes into custody an individual whom the officer believes, because of the age of the child, may be enrolled in a primary or secondary school as provided by Chapter 52 of the Texas Family Code shall do the following:
  - a. Attempt to determine if the individual is a student.
    - i. If the individual is known to or believed to be enrolled in a school, and
    - ii. The child's alleged offense is an offense under section: 19.02, 19.03, 19.04, 19.05, 20.02, 20.03, 20.04, 21.08, 21.11, 22.01, 22.011, 22.02, 22.021, 22.04, 22.05, 22.07, 28.02, 29.02, 29.03, 30.02, or 71.02, Penal Code, or
    - iii. The Unlawful Use, Sale or Possession of a Controlled Substance, Drug Paraphernalia, or Marijuana, as defined by Chapter 481, Health and Safety Code; or
    - iv. The Unlawful Possession of any of the Weapons or Devices listed in Section 46.01(1)-(14) or (16), Penal Code; or a Weapon listed as a Prohibited Weapon under Section 46.05, Penal Code; or
    - v. Any felony offense.
  - b. If the individual meets these requirements the officer or detective assigned shall give oral notification to the superintendent or the designee of the public-school district within 24 hours after the arrest or detention of a child, or on the next school day.
  - c. Written notification shall be mailed within seven (7) days after the date of oral notification to the appropriate afore-mentioned school official, marked "Personal and Confidential" on the mailing envelope.

2. The complete text of this responsibility is found in Article 15.27 Code of Criminal Procedures.

E. Juvenile Records (TEXAS BEST PRACTICES 10.02f)

1. The computerized Juvenile Justice Information System (JJIS) is designed to track juvenile cases from intake through detention, prosecution, and case disposition, including probation or commitment. The Texas Family Code restricts entries into the JJIS to delinquent conduct offenses that, if committed by an adult, would be punishable by jail or imprisonment.
  - a. JJIS entries are made on Teague Police Department detentions by the Juvenile Investigation Division when a juvenile is referred to the juvenile court.
  - b. JJIS records may be accessed and disseminated according to the same rules that apply to computerized criminal histories.
  - c. JJIS entries cannot be made for juveniles who are not referred to the juvenile court within 10 days of the detention.
  - d. Records that do not qualify for JJIS entry are to be destroyed.
2. Texas Family Code requires that local law-enforcement records and files concerning a juvenile must be kept separate from adult files and records and prohibits them from being sent to a central state or federal depository except as specified in the Texas Family Code. Juvenile detention reports will be separated from adult arrest reports as required by the statute.
  - a. Records or files that are required or authorized to be maintained under laws regulating operation of motor vehicles and records that list a juvenile as the victim of a criminal offense are specifically exempt from the file- separation requirement.
  - b. Reports of missing juveniles are specifically authorized to be entered into TCIC and NCIC.
3. The Code of Criminal Procedure authorizes information on juveniles to be included in a local system for the purpose of investigating or prosecuting the criminal activities of criminal combinations. This information may be released to another criminal justice agency, a court, or a defendant in a criminal proceeding pursuant to the discovery. The record must be destroyed no later than two years after its collection if the juvenile has not been charged with criminal activity.
4. The preservation and destruction of juvenile records is the responsibility of the juvenile investigation division. Juvenile records will be kept under lock and key and access will be limited to juvenile investigators.

5. The Texas Family Code prohibits taking photographs or fingerprints of a juvenile without the consent of the juvenile court or the juvenile probation officer unless the juvenile is taken into custody for a felony or a misdemeanor punishable by confinement in jail. Only the procedures specified in these General Orders will be utilized.
6. Release of Information on juvenile offenders may only be made pursuant to the following:
  - a. A written request under the Texas Public Information Act, Government Code Chapter 552 to the police department as approved by the city attorney or to the Teague Municipal Court for fine-only offenses handled there.
  - b. The Sex Offender Registration Act, Code of Criminal Procedures Chapter 62. The request must be made in writing and will be responded to by the police department.
  - c. Code of Criminal Procedures Article 15.27. Notice to schools of specified offenses committed by students. These notices will be made by assigned officers.

	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 7.13 Domestic Violence and Protective Orders</b>
	<b>Effective Date: November 15, 2021   Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>
	<b>Reference: Texas Best Practices 7.08</b>

**I. POLICY**

The department assigns domestic or family violence (domestic disturbance) calls a high priority. The nature and seriousness of crimes committed between family or household members are not mitigated because of the relationships or living arrangements of those involved. Law enforcement agencies must exercise leadership in the community in responding to domestic violence. An immediate criminal justice response can make a major difference in the disputants' lives. With all due consideration for their own safety, department personnel responding to a domestic disturbance call shall (1) restore order, (2) arrest persons when probable cause exists that a crime has been committed, (3) provide safety and security for the crime victim(s), and (4) help participants contact appropriate agencies that might help prevent future occurrences.

**II. PURPOSE**

To define domestic violence and related offenses, outline a safe procedure for handling violent incidents and calls, and describe measures that can be taken to end violence and protect victims.

**III. DEFINITIONS**

- A. Assault: An act by an assailant who intentionally, knowingly, or recklessly causes bodily injury to another, including the person’s spouse. A threat to cause imminent bodily injury to another, including the person’s spouse, is also an assault. This definition is not all-inclusive as family violence may also entail aggravated circumstances, sexual assault, and other offenses. The assault definition also extends to intimate partner violence (IPV) that includes unmarried couples. See Chapter 22 and 25 of the Texas Penal Code.
  
- B. Domestic violence shelters/programs: Services that are provided (usually 24 hours a day) for women and their children who have been physically or emotionally abused, or who have been threatened with abuse by their spouses or partners. Services include crisis intervention, counseling, shelter, escort to court, food, clothing, and transportation. Some shelters also provide information pertaining to jobs, social

security services, restraining orders, and various other items of information that is needed if the victim does not wish to return to the previous situation.

- C. Family violence: An act by a member of a family or household against another member of the family or household that is intended to result in physical harm, bodily injury, assault, or sexual assault or that is a threat that reasonably places the member in fear of imminent physical harm, bodily injury, assault, or sexual assault, but does not include defensive measures to protect oneself.
- D. Abuse: as defined by Sections 261.001(1) (C), (E), and (G) by a member of a family or household toward a member of the family or household.
- E. Dating Violence: as defined by Section 71.0021.
- F. Family or household member:
  - 1. Spouses, whether residing in the same home.
  - 2. Former spouses, whether residing in the same home or not.
  - 3. Persons who have a child in common, whether they have ever been married or resided together.
  - 4. Parents, children, stepparents, stepchildren, grandparents, grandchildren, brothers and sisters, half-brothers and half-sisters, regardless of whether they reside in the same home with the suspect.
  - 5. Parents-in-law, children-in-law, brothers- and sisters-in-law regardless of whether they reside in the same home with the suspect.
  - 6. Persons, whether related or not, who cohabit or who previously cohabited with the suspect, and any children of either who then resided in the same home as the suspect.
  - 7. See Sections 71.003, 71.004, and 71.005 of the Family Code.
- G. Protective order, sometimes referred to as a “restraining order:” A court order of protection on behalf of an abused family/household member that restrains the abuser from further acts of violence, may order the abuser to refrain from further contact, vacate the residence, relinquish custody of a vehicle, provide temporary child support, plus other measures. A protective order may be valid up to two years.

Types of protective orders:

- 1. Emergency protective order: A protective order issued by a magistrate to a defendant following his or her arrest for an act of family violence. The EPO



may be applied for by the victim, a police officer, or may be issued on the magistrate's own motion. The victim may request the EPO at the scene of a domestic violence incident.

2. Protective order: A protective order that is requested by a victim of family violence at any time other than at the scene of a domestic violence incident.
3. Temporary Ex Parte Orders: an order that is issued without the person who committed family violence present. A person subject to an order (the actor) who violates an Ex Parte order may not be arrested unless it is established that the actor had been served with the order prior to the commission of the act(s) violating the order. If an officer arrives and the actor is not aware of the order, the officer may assist the protected person in informing the actor of the existence of the order. The protected person should provide the actor with a copy of the order if possible. The officer shall then remain at the scene until the actor has complied with any wording that requires him or her to leave the residence. If the order does not require the actor to leave, the officer shall remain at the scene while the protected person gathers necessary items to leave. See Texas Family Code Chapter 83 for additional information.

#### **IV. PROCEDURES: General responsibilities**

- A. Department personnel shall refer victims of domestic violence or serious bodily injury crimes to appropriate community resources (mental health agencies, medical doctors, legal assistance agencies, victim/witness assistance programs, domestic violence shelters/programs, and the County Attorney's Office), and shall provide victims with the name, address, and telephone numbers of the county attorney and the investigating law enforcement agency. Where possible, officers shall help victims directly access referral agencies.
- B. Department personnel shall be trained about domestic violence and its impact. Officers are encouraged to consult community resources, such as the local domestic violence shelter and the local victim/witness advocacy program.
- C. Personnel must be well trained in how to confront unexpected violence. Disturbance calls can be dangerous to responding officers.

#### **V. PROCEDURES - Patrol responsibilities**

- A. Before arrival at the scene officers should do the following:
  1. Obtain all available information from the dispatcher before arrival.
  2. When possible, officers should wait for back-up help, discuss a strategy, and approach the dispute scene in pairs.

- B. Near the scene officers should avoid the use of sirens and other alarms. The suspect might be dangerous and could turn a weapon on arriving officers.
- C. At the scene, the officer should observe the location of the dispute before contacting the complainant. Consider the surroundings. Park the marked car a short distance away. Each officer should follow a separate approach to the scene of the dispute, maintaining maximum cover and an escape route. From this point on, officers should remain within sight of one another, if possible.
- D. Before knocking on the door, officers should listen, and they should look in windows to obtain additional information about the situation (e.g., layout of the house, number of people, weapons, evidence of violence or damage).
- E. Officers must be concerned for their own safety as well as that of the disputants. To minimize the possibility of injury, stand to the side of the door and not in front of windows when knocking. The unexpected may occur when the door opens.
  - 1. Initial contact with occupant(s).
    - a. Identify themselves as law enforcement officers by name, explain your presence, and request entry into the home (when conditions permit). Ascertain identity of complainant and ask to see him or her and any other person at the home.
    - b. Officers shall not accept statements from any disputant or witness that the call was a mistake without investigating further.
    - c. Officers shall make every reasonable effort to interview the complainant and remain on scene to assess welfare and safety as required by training and experience.
    - d. If entry is refused, officers must explain that they must make sure there are no injured persons inside. If no one responds to knocking, officers shall try to establish voice contact by shouting for an answer.
    - e. Refusal of entry or no response to a knock at the door will require a forced entrance only if officers have a reasonable belief that person(s) inside are at risk of imminent death or serious bodily injury.
    - f. Officers may conduct a search of the premises if consent has been given to do so. Although a consent search eliminates the need for a warrant and for probable cause, such consent must be freely and voluntarily given. If two people have joint ownership or possession of a place or thing, either one may give a valid consent. However, the other, if present, may legally object. Once a party refuses consent, officers must obtain a warrant to search or articulate another exception to the warrant requirement.

- g. A spouse or cohabitant can consent to the search of premises used jointly by both husband and wife or by unmarried cohabitants. However, if both are present, either one may legally object. Once either party refuses consent, officers must obtain a warrant to search or articulate an exception to the warrant requirement.
- F. Officers may also make a warrantless entry to conduct a search if an emergency exists. Officers must have a reasonable belief that such an emergency does exist. For example, if officers believe that someone, perhaps a child or spouse, needs emergency assistance they may search the premises without a warrant.
- 1. Officers shall evaluate the following elements when considering a warrantless entry:
    - a. The degree of urgency involved, and the time required to get a warrant.
    - b. The possibility of danger to occupants of the house or others, including officers guarding the site.
    - c. Whether the suspected offense is serious and involves violence.
    - d. Whether officers reasonably believe that persons may be armed.
    - e. Finally, officers are reminded that they have a lawful right and duty to investigate any situation that they reasonably believe to be an emergency.
  - 2. Once inside, establish control by:
    - a. Inquiring about the nature of the dispute.
    - b. Identifying disputants.
    - c. Being aware of potential weapons in surroundings.
    - d. Determining if persons are in other rooms, whether children or adults, and the extent of any injuries. (These persons should be separated from the parties involved and kept out of hearing range, so their status as possible witnesses will not be compromised.)
    - e. Protect the victim from further abuse. Separate the victim from the suspect and arrange for medical attention if the victim is hurt. If the victim appears injured and yet refuses medical assistance, carefully document any observed injuries, as well as the refusal of medical treatment. Photograph the victim's injuries if possible.
    - f. Ascertain whether a protective order has been violated.

- g. If weapons -- firearms, knives, or any other object that could be used as a weapon-- are present, secure them away from the disputants, if practicable, while the disputants are being interviewed. If appropriate, seize weapons for evidence.
  - h. Transporting family/household members to a hospital, a safe shelter, or a magistrate.
- 3. Officers shall transport victims to a safe location as they wish or as the circumstances require.
  - 4. If a complainant seeks officers' help in entering his or her residence to obtain personal property, the officers must determine that the complainant has lawful authority to do so; must advise all parties that they are accompanying the complainant to obtain items for immediate personal (or children's) use; that the officers' function is to maintain order; that any dispute over property is a matter for the courts to decide.

**NOTE:** Texas statutes afford officers liability immunity only in cases which they provide a civil standby in cases of domestic violence (CCP Article 5.045). There is no requirement in statute that this service is performed, as it is discretionary duty. Officers shall contact a supervisor, review the situation, and only conduct a civil standby with supervisory approval.

#### G. Interviewing all disputants

- 1. Ensure safety and privacy by interviewing the victim in a place separate from the suspect, assuming the suspect has been identified.
- 2. Critical to the success of the interview is the officer's manner. Officers must listen, show interest in the disputants and their problem, and remain aware of nonverbal communications signals.
- 3. Officers shall attempt a low-key approach in domestic violence cases. Maintain good eye contact through natural, spontaneous glances. (Fixed gazes or staring increase fear and hostility.) A relaxed stance and appropriate facial and head movements demonstrate interest and encourage the victim to continue speaking.
- 4. If possible, separate the parties so that they can individually describe the incident without interruption. (This may help the parties relieve emotional tension.) Although the disputants are to be separated, officers shall remain within sight and hearing of each other.

5. After the parties have given their statements, the officers should ask about details for clarification, and summarize the stated accounts, giving the parties an opportunity to point out anything that might be misrepresented.
6. Officers should be aware that verbal statements made by parties have evidentiary value. All verbal statements should be recorded, when practicable, and should be noted in reports of the incident.
7. Interviewing the victim. Get answers to the following questions from the victim:
  - a. What happened?
  - b. Were there any injuries and who caused them?
  - c. What weapons or objects were used?
  - d. What is the relationship to suspect?
  - e. Were threats made against the victim or others?
  - f. Was there forced sexual contact.
  - g. Are there any court cases pending against suspect?
  - h. Are any protective orders in effect.
  - i. Is suspect on probation or parole?
  - j. Did the suspect threaten or hurt others, particularly children or pets?
  - k. Was property damaged and if so, what was the damage?

#### H. Interviewing witnesses

1. Interview any witnesses to the incident--children, other family members, neighbors--as soon as possible.
2. Remember that witnesses may be experiencing significant emotional crises that might influence the accuracy of their accounts.
3. If witnesses provide information about prior assaults, document them to help establish a pattern.
4. Children of disputants should be interviewed with care and kindness. Sit, kneel, or otherwise be at their level when speaking to them. Signs of trauma or abuse should be noted.

## I. Collection of Evidence

Officers should treat a family violence offense with the same seriousness as other criminal offenses, and conduct a preliminary investigation in the same manner to include:

1. Collecting any physical evidence or calling crime scene personnel to do so.
2. Photographing any damages or injuries received by any party involved in the incident.

## VI. PROCEDURES - Arrests

- A. Officers shall make an arrest without a warrant if they have probable cause to believe that the individual has committed an assault resulting in bodily injury to a member of the person's family or household. Further, the department promotes a policy of arrest when the elements of an appropriate offense are present, persons who the peace officer has probable cause to believe have committed an offense involving family violence.
- B. If officers cannot identify a predominant physical aggressor and do not make an arrest, they shall nevertheless thoroughly document the incident.
- C. Officers shall not threaten to arrest all parties involved for the purpose of discouraging future requests for law enforcement intervention.
- D. If the victim claims that a protective order has been violated, officers shall review the victim's copy of the order, checking it for validity. If a protective order exists and its terms ("no contact," "no trespass," or "no further abuse") have been violated the officer shall arrest the violator, assuming probable cause exists.
- E. Officers making arrests for family violence may petition for an emergency protective order, if requested by the victim or if the officer believes there is a significant danger of future assaults.
- F. Officers shall contact Child Protective Services worker if a child is abused or if neither parent can reasonably look after the child's safety and well-being. (Child neglect is a separate, reportable offense.)
- G. In determining probable cause, the officer shall NOT consider:
  1. Race, sex, ethnicity, social class, or sexual orientation.
  2. Whether the complainant has not sought or obtained a protective order.

3. The officer's own preference to reconcile the parties despite the complainant's insistence that an arrest be made.
  4. That the complainant has called for law enforcement protection previously and has not pursued or has withdrawn the criminal complaint against the abuser.
  5. That the complainant has not begun divorce proceedings.
  6. Assurances of either or both disputants that violence will stop.
  7. The lack of visible bruises or injuries.
- H. Factors favoring the decision to arrest based upon probable cause that an offense has been committed
1. Arrest is the most appropriate response when these factors are present:
    - a. Serious, intense conflict.
    - b. Use of a weapon.
    - c. Previous injury or damage.
    - d. Previous court appearance against the offending party.
    - e. Previous attempt to sever the relationship.
    - f. Previous calls for law enforcement help.
    - g. When a felony has occurred.
    - h. Evidence of drugs or alcohol use at the assault.
    - i. Offenses committed with the officer present.
    - j. Valid warrants on file for other crimes.
    - k. Officers shall arrest for a violation of a protective order committed in the officer's presence or view.
    - l. Aggressive behavior toward any person or pets, or any other threatening behavior.
- I. If the abusive person is to be arrested, the officer should use the following procedure:

1. If the suspect is present, arrest him/her, apply handcuffs, inform him/her that the decision to arrest is a law-enforcement one, and transport securely to the jail/magistrate.
  2. If the suspect is absent or has been arrested, transport (or arrange transportation for) the victim to a safe shelter or other appropriate place. Circulate a "be-on-the-lookout" message describing the suspect, if necessary, and arrange for an arrest warrant.
  3. If an arrest must be made because a protective order has been violated, verify its validity by:
    - a. Examining the victim's copy, if available.
    - b. Having communications search TCIC or contact the jurisdiction that issued the order to confirm its currency.
- J. If the abusive person is not arrested, the officer should use the following procedure:
1. Complete an incident report and give a copy or arrange to have a copy given to the victim.
  2. Inform the victim that the department will begin action to procure a warrant for the offender if an offense occurred.
  3. Advise the victim of the importance of preserving evidence.
  4. Explain to the victim about protective orders and how to obtain them and offer to help the victim obtain them later.
  5. If the victim wants to leave the premises to ensure safety, remain at the scene while the victim packs essentials. Advise the victim to take only personal items plus important papers, such as a marriage license or divorce decree, health insurance cards, and if children are involved their school records, proof of vaccination, and health information.
  6. Regardless of whether an arrest is made, the officer shall provide the "Notice to Adult Victims of Family Violence" to the victim, which explains legal and community resources available, including the name, address, and telephone number of the county attorney and the investigating law enforcement agency.
  7. Assure the victim that Teague Police Department shall assist in future emergencies and explain measures for enhancing his/ her own safety.



- K. Gathering evidence. Physical evidence takes three forms in domestic violence cases: the injuries sustained by the victim, evidentiary articles that substantiate an attack, and the crime scene itself. The on-the-scene officer should take the following actions:
1. If possible, have a physician corroborate the victim's account of injuries sustained. Since choking is one of the most serious forms of violence but is sometimes hardest to detect, the officer and/or the physician should take note of that. Officers should document these cases on a strangulation supplemental report, in addition to their offense reports.
  2. When feasible, take photographs of injuries.
  3. Photograph the crime scene to show that a struggle occurred; if photography is not possible, write a description of it.
  4. Collect evidence according to the same principles applied to any other crime scene.
  5. Seize any weapons that the predominant physical aggressor used or threatened to use in the commission of any crime.
  6. Obtain statements from all witnesses, particularly noting any verbal statements that bear on the incident. Officers shall note the emotional state of the person making the verbal statement.
- L. Documenting the incident. All incident reports on domestic violence shall follow general reporting procedures. Officers should include the following in their reports:
1. Facts and circumstances of domestic violence including a description of why one disputant was deemed the predominant physical aggressor.
  2. Victim's statements as to the frequency and severity of prior incidents of abuse by the same family or household member.
  3. The victim's statements as to the number of prior calls for law enforcement assistance.
- M. The disposition of the investigation. Officers involved in an incident should do the following:
1. Thoroughly document probable cause to arrest.
  2. If an arrest is not made for domestic violence, the incident must still be documented, stating that either no probable cause for arrest existed, or circumstances dictated another course of action. In such cases, in addition to the above considerations, officers shall note:

- a. What referral information was given.
  - b. The name of any counselor contacted.
  - c. Why no arrest was made, nor any warrant issued.
3. If children were present, make a report of abuse or neglect, if appropriate, and forward it to Child Protective Services.
  4. Regardless of whether an arrest is made, the officer shall provide the “Notice to Adult Victims of Family Violence” to the victim, which explains legal and community resources available, including the name, address and telephone number of the county attorney and the investigating law enforcement agency.

N. Arrests of agency personnel

1. If the predominant physical aggressor or abuser is an employee of this agency or the City of Teague, the responding officer shall summon a supervisor, who shall in turn notify the Chief of Police.
2. The scene shall be secured and, if required, summon emergency medical services. The employee shall be disarmed or removed from access to weapons. The possibility exists that the employee's departmental weapon may be evidence of an offense.
3. A supervisor shall be summoned who shall begin an internal criminal investigation:
  - a. If probable cause to arrest exists, the supervisor shall arrest and gather evidence (including taking photographs) consistent with this general order.
  - b. The supervisor shall work with the responding patrol officer to ensure that the victim receives medical attention, if necessary, is transported to a hospital or safe shelter, and that all reports are completed, evidence gathered, and photographs taken. The responding patrol officer shall assist in obtaining an emergency protective order.
  - c. The supervisor shall speedily present the case to the county attorney.
4. Upon termination of the criminal investigation, the Chief of Police may assign an officer to undertake an internal administrative investigation into the incident. The chief may suspend the employee pending the outcome of the investigation.
  - a. Suspended employees shall immediately turn in all agency-issued weapons, vehicles, badges, and identification.

- b. If the internal administrative investigation supports a violation of agency policy, the Chief of Police shall take appropriate action. Further, if the investigation confirms that domestic violence occurred, the Chief of Police may require that the officer receive counseling, psychological evaluation, demotion, or termination of employment.
- c. Federal law states that any person (including a law- enforcement officer) convicted under any state or federal law for a misdemeanor involving the use of, attempted use of physical force, or the threatened use of a deadly weapon when committed by a current or former spouse, parent or guardian of the victim, a person sharing a child in common, or a cohabitant of the victim (past or present), is prohibited from shipping, transporting, possessing, or receiving firearms or ammunition. The offense may have occurred at any time. Law enforcement officers convicted of offenses involving weapons or threats of force may, therefore, be unable to maintain their certification.

**Note:** that officers who are the subject of a protective order shall not carry firearms. Officers who are the subject of a protective order shall turn in all agency-issued weapons.

## **VII. PROCEDURES - Issuing an emergency protective order**


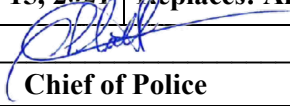
### **A. Emergency protective orders (EPO) (domestic violence)**

- 1. Officers shall complete a magistrate information sheet for all Family Violence cases. This sheet shall be included with the case report. This sheet shall be included with the original warrant of arrest, in cases that officers attain an arrest warrant, and delivered to the Freestone County Sheriff's Office with the warrant.
- 2. The EPO aims to protect the health or safety of a victim of domestic violence. It is issued only if the offender is arrested. The judge or magistrate who arraigns the offender after the arrest may issue the EPO on the magistrate's own initiative, upon request of the victim, the guardian of the victim, a peace officer, or an attorney representing the state. If an officer has at least a reasonable belief that an assault has occurred and there exists probable danger of further abuse, the officer shall request the judge or magistrate to issue an EPO.
  - a. If circumstances make it impossible or inappropriate for an officer to obtain the EPO, the officer shall advise the victim that he/ she can request an EPO directly from a magistrate or the county attorney.
  - b. The victim does not need to press charges or swear a warrant. The presence of the victim or suspect is immaterial to obtaining an EPO.

- c. An EPO may order a stop to abusive behavior, prohibit contact between parties, order the abuser out of a shared home, or deny the abuser the right to possess a firearm, and provide other relief.
3. An officer can petition for an EPO by telephone or in person.
4. The EPO remains in effect for up to 61 days but not less than 31 days. The victim can petition for a permanent protective order before the expiration of an EPO.
5. The offender is served with a copy of the order at the time of arraignment. The victim will be contacted and informed that an EPO has been issued and will be provided with a copy and informed of its requirements.
6. A copy is also delivered to the Chief of Police and the communications center for the jurisdiction where the victim resides.

#### B. Protective Orders from Other States

Officers shall enforce protective orders from other states or possessions of the United States as if they were issued in Texas. This applies to all orders in which the respondent has received notice and opportunity to attend a protective order hearing. Enforcement of out-of-state protective orders does not require that they be registered in Texas. If officers are unable to verify an outstanding protective order, they must nevertheless honor it. Officers cannot arrest for violation of the order, however, if the violator has not been served with it.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.14 Vehicle Operation</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 7.15, 7.20, and 7.24	

## I. POLICY

All personnel operating department vehicles shall exercise due regard for the safety of all persons. Protection of life is the paramount goal of the department. No task, call, or incident justifies disregard of public safety. Further, the public expects its law-enforcement officers to demonstrate exemplary driving skills. All department personnel who operate department vehicles will comply with the safe-driving procedures outlined in this policy with attention to responding to calls for service or engaging in pursuits. Emergency warning devices shall be used consistent with both legal requirements and the safety of the public and department personnel.

## II. PURPOSE

The purpose of this policy is to establish procedures governing the operation of police vehicles.

## III. DEFINITIONS

- A. **Emergency driving.** Driving in response to a life-threatening or other serious incident (based on available information) that requires emergency equipment. Emergency driving -- with emergency lights and siren activated -- allows an officer to disregard traffic regulations, but officers must still drive with due regard for the safety of the officer and others.
- B. **Emergency equipment.** Emergency lights and a siren, whistle, or air horn designed to give intermittent signals automatically. All marked vehicles have distinctive, reflectorized decals for additional visibility. In this order, an authorized emergency vehicle is one that has this emergency equipment installed.
- C. **Normal or routine driving.** Driving that dictates vehicle speed consistent with the normal flow of traffic, obedience to vehicle laws and posted signs, and adherence to commonly understood "rules of the road."

### III. GENERAL PROCEDURES FOR ALL RESPONSES (TEXAS BEST PRACTICES: 7.15)

#### A. General

1. All departmental vehicles shall be driven safely and properly in full compliance with all traffic laws and regulations. Department vehicles are conspicuous symbols of authority on the streets and many people observe an officer's actions. Each officer must set an example of good driving behavior and habits.
2. Under certain emergencies as defined below, the Transportation Code authorizes officers to disregard traffic regulations. Both the operator and the department, however, are not released from civil liability for failure to use reasonable care in such operations.

#### B. Routine operation

1. In case of accident or damage to any department vehicle, the driver shall immediately notify a supervisor, so an administrative investigation may be conducted.
2. Accidents involving members of this department will be investigated by Texas Department of Public Safety.
3. Drivers involved in an accident shall write a memorandum, directed through the chain of command to the Chief of Police, detailing the circumstances.
4. Drivers shall report any found damage or other non-accident damage to their supervisor immediately and document the damage in an incident report.
5. Vehicles used in routine or general patrol service shall be conspicuously marked except those being used for covert patrol operations.
6. Unmarked cars shall not be used in any pursuit but may be used for patrol.
7. Unmarked cars that are provided with emergency lights and a siren may be used to stop vehicles.
8. Standard lighting equipment on marked vehicles includes hazardous warning lights, spotlights, and alley (side) lights on the rooftop light bar.
  - a. Hazardous warning lights may be used at any time the department vehicle is parked where other moving vehicles may be endangered.
  - b. Alley lights and spotlights may be used when the vehicle is stationary or moving at speeds not to exceed 15 miles per hour and shall not be used in a manner that will blind or interfere with the vision of operators of approaching vehicles.
9. Seat belts and shoulder straps shall be worn by the driver and all passengers during vehicle operation. Prisoners shall be strapped in with seat belts whenever possible. (TEXAS BEST PRACTICES: 7.20)

Exception: When approaching an incident scene or a call where the officer believes that a rapid exit from the vehicle may be required, the officer may release his/her seat belt.

10. Any young children transported in a police vehicle will be transported in the manner prescribed by the Transportation Code using infant/child car seats when necessary.

#### C. Inspection (TEXAS BEST PRACTICES: 7.24)

1. Before each duty assignment, officers shall check their vehicles for cleanliness, operability, and all required equipment.
2. Officers shall also ensure that vehicles have adequate levels of oil, brake fluid, power steering fluid, and gas. Any deficiencies should be reported to the supervisor.
3. Officers shall check the safety features of the vehicle before assuming duty. The check shall include, but is not limited to, all lights, brakes, siren, horn, and steering.
4. Officers shall also check tires for tread wear and proper inflation.
5. Officers shall examine their vehicles at the beginning and the end of their shifts for damage. Officers shall report any damage immediately to supervisor.
6. Officers shall examine their vehicles at the beginning and end of their shifts to search for evidence, contraband, or property discarded by prisoners or others. Rear seats shall be thoroughly checked.
7. Officers who discover a department vehicle in need of repairs shall document the need on a vehicle inspection sheet and inform the supervisor.
8. If, in the opinion of the Chief of Police, vehicle damage resulted from abuse or neglect caused by an officer, disciplinary action may result.
9. No driver shall modify, remove, de-activate, or otherwise tamper with the vehicle safety belts, emission control device, or any part of the vehicle that affects its operation.
10. Officers are responsible for maintaining the cleanliness of the interior and exterior of their assigned vehicle. During periods of inclement weather when department vehicles cannot be washed regularly, the driver must ensure that headlight and taillight lenses are kept clean, insofar as circumstances permit.
11. No officer or employee shall operate any department vehicle that he or she believes is unsafe.

#### D. Driving rules

1. The driver shall carefully observe the surrounding conditions before turning or backing any vehicle.
2. A department vehicle shall not be left unattended with the engine running, except when handling a call for service and the vehicle has been locked.
3. The driver must recognize the variable factors of weather, road surface conditions, road contour, and traffic congestion, all of which directly affect the safe operation of any motor vehicle and shall govern the operation of the vehicle accordingly.
4. Emergency driving to the scene of a motor vehicle accident is permissible only when an emergency exists, when specific information indicates that conditions at the scene require an emergency response, or when directed to do so by a supervisor.
5. Upon approaching a controlled intersection or other location where there is possibility of collision because of traffic congestion, the emergency driver shall reduce the speed of the vehicle, stopping completely if necessary, before entering and traversing the intersection. When faced with a red traffic signal or stop sign, the officer shall stop his or her vehicle and ensure by careful observation that the way is clear before proceeding through the intersection.

\*NOTE: Officers should bear in mind that driving with lights and sirens is not a command of authority to disregard traffic law, rather they are warning the public and requesting permission to traverse intersections against traffic laws.

6. Regardless of the seriousness of the situation to which the officer is responding, excepting circumstances that are clearly beyond the officer's control, he or she shall be held accountable for the way he or she operates the vehicle.
7. At the scene of a crime, a motor vehicle crash, or other incident, a department vehicle shall be parked in such a manner so as not to create an obstacle or hazard to other traffic, unless necessary for the protection of an incident scene or injured persons. If a traffic hazard exists, the emergency lights shall be used to warn other drivers approaching the location.
8. Operators of department vehicles must bear in mind that the traffic regulation requiring other vehicles to yield the right of way to any emergency vehicle does not relieve emergency vehicle operators from the duty to drive with due regard for the safety of all persons using the highways. Nor does this traffic regulation protect the driver from the consequences of arbitrary use of this right-of-way regulation.

#### **IV. PROCEDURES FOR EMERGENCY DRIVING**

##### **A. General**

1. No fixed rule can apply to every circumstance that may arise governing emergency driving. Although an officer may receive information that leads him/her to respond to a call with emergency lights and siren activated, in the majority of such cases an officer discovers, upon arrival, that an emergency response was not justified.



2. Section 546.005 of the Transportation Code states that the exemptions to driving laws granted to emergency vehicle operators "does not relieve the operator from the duty to drive with appropriate regard for the safety of all persons or the consequences of reckless disregard for the safety of others." Recognizing that protection of human life is paramount, responding officers must remember that their objective is to get to the location of the occurrence as soon as possible--safely--without danger to themselves or to others.

B. Response codes: Calls for service are classified as Code 1 or Code 3, depending on circumstances. The codes are defined as follows:

1. Code 1 responses are utilized for any situation regardless of apparent urgency where the preservation of life is not a consideration. Units responding to Code 1 calls shall respond to the location without delay, complying with all traffic regulations, and shall not use emergency warning devices.
2. Code 3 responses are authorized for any emergency where the preservation of life is a consideration. Primary and support units responding to Code 3 calls shall proceed rapidly to the location of the emergency by the most direct means, using all emergency warning devices with a paramount consideration for the safety of the public and the assigned officers. Supervisors shall closely monitor all Code 3 calls and shall respond if necessary.

NOTE: Supervisors shall monitor the response codes for calls for assistance and shall have the authority to upgrade or downgrade assigned response codes.


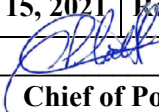
C. Officer's response to call

1. Upon arrival at the scene of a call, the responding officer shall rapidly evaluate the situation and determine whether additional units are still needed or whether other units responding Code 3 can be slowed or cancelled.
2. All units responding to robbery-in-progress and burglary-in-progress calls, before coming within hearing distance, shall discontinue the use of the siren and at that time fully comply with all traffic laws. Before coming within sight of the location, officers shall discontinue the use of the emergency warning lights. Officers are reminded that upon deactivation of a siren and flashing lights, their response ceases to be an emergency and they must comply with all posted speeds and traffic control devices.
3. In situations requiring a silent response, e.g., alarms and prowler calls, officers shall respond as rapidly as possible, obeying all traffic laws and signs.
4. Officer-initiated response.
  - a. When, in the opinion of the officer, an emergency is imminent or exists, or that activation of emergency warning devices is necessary to protect life or render the necessary enforcement, the department authorizes an emergency response.

- b. Examples include the following:
  - i. Any incident where the use of emergency lights constitutes a necessary warning for the safety of life (such as scenes of fires, accidents, or disasters).
  - ii. As a visual signal to attract the attention of motorists being stopped for traffic violations, or to warn motorists of imminent dangers.
  - iii. Responding to Code 1 calls, where the officer has previous or additional information.
  - iv. Where because of location, distance to be traveled, or traffic conditions, the officer determines that emergency operating conditions are essential to provide an appropriate response.
  - v. In response to an officer's emergency request for assistance.
  - vi. For pursuit. (See Policy 7.15)

D. Use of emergency warning devices in non-emergencies

- 1. Officers shall activate emergency equipment to notify drivers that they must stop, and to provide a safe environment for the driver, officer, and the public.
- 2. Officers may activate emergency equipment in non-emergencies when expediency is required to eliminate a potential hazard to the public or other officers, such as using emergency lights to protect disabled motorists or when department vehicles are used as protective barriers.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.15 Vehicle Pursuits</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 7.13, 7.14, 7.18, and 7.19	

## I. POLICY

Pursuits represent a dangerous and difficult task that receives much public and legal scrutiny when accidents, injuries, or death result. Pursuing officers and supervisors must justify their actions and, once they have decided to pursue, they must continuously evaluate the safety of their actions. Further, forcible measures to stop a fleeing driver, as detailed below, are prohibited except where deadly force is appropriate.

Officers shall comply with all applicable portions of Policy 7.15 when they are involved in vehicle pursuits.

## II. PURPOSE

The purpose of this policy is to establish procedures governing the operation of police vehicles, with special attention to emergencies and pursuits.

## III. DEFINITIONS

- A. **Boxing in:** A deliberate tactic by two or more pursuit vehicles to force a pursued vehicle in a specific direction or to force it to reduce speed or stop by maneuvering the pursuit vehicles in front of, behind, or beside the pursued vehicle.
- B. **Caravanning:** Direct participation in a pursuit by department vehicles other than the primary and authorized support vehicles.
- C. **Emergency driving:** Driving in response to a life-threatening or other serious incident (based on available information) that requires emergency equipment in operation.
- D. **Emergency equipment:** Emergency lights and a siren, whistle, air horn or any other equipment designed to give intermittent signals automatically. All marked vehicles have distinctive, reflectorized decals for additional visibility. In this order, an authorized emergency vehicle is one that is equipped with emergency equipment.
- E. **Normal or routine driving:** Driving that dictates vehicle speed consistent with the normal flow of traffic, obedience to vehicle laws and posted signs, adherence to commonly understood "rules of the road."

- F. Primary pursuit vehicle: Normally the department vehicle that begins the pursuit or the vehicle closest to the fleeing suspect. The primary pursuit vehicle may be re-designated by order of a supervisor.
- G. Pursuit: An active attempt by an officer in an authorized emergency vehicle to apprehend a suspect who is fleeing or evading apprehension, provided the officer reasonably believes that the suspect is refusing to stop and is willfully fleeing capture by high-speed driving or other evasive maneuvers. Pursuits shall be conducted only with activated emergency equipment and under circumstances outlined in this order.
- H. Not a pursuit: An attempt to stop a vehicle that is not fleeing, or an attempt to stop a vehicle that is refusing to stop while still obeying traffic-control devices and not exceeding the speed limit by more than ten miles per hour is not a pursuit.
- I. Risk: The degree of danger or hazard to the public or officers.
- J. Roadblock: Any method, restriction, or obstruction used to prevent free passage of vehicles on a roadway in order to stop a suspect.
- K. Support vehicles: The second or additional department vehicles participating in the pursuit that follow the primary pursuit vehicle at a safe distance. Once the vehicles have stopped, officers in the support vehicles can provide help for the officer in the primary vehicle or they can assume the primary role if circumstances dictate.

#### **IV. PROCEDURES FOR PURSUITS (TBP: 7.13)**

- A. Justification for pursuit:
  - 1. Any law enforcement officer in an authorized emergency vehicle may initiate a vehicular pursuit when the suspect exhibits the intention to avoid apprehension for a felony or misdemeanor that would result in jail by refusing to stop when properly directed to do so. Pursuit may also be justified if the officer reasonably believes that the suspect, if allowed to flee, would present a danger to human life or cause serious injury.
  - 2. Pursuits will not be initiated for class C traffic offenses alone.
  - 3. The decision to initiate pursuit must be based on the pursuing officer's conclusion that the immediate danger to the officer and the public created by the pursuit is less than the immediate or potential danger to the public should the suspect remain at large.
  - 4. In deciding whether to initiate pursuit, the officer shall take the following into consideration:
    - a. road, weather and environmental conditions;

- b. risk of harm to the public as assessed by population density and vehicular and pedestrian traffic;
- c. the relative performance capabilities of the pursuit vehicle and the vehicle being pursued;
- d. the seriousness of the offense;
- e. the presence of other persons in the police vehicle;
- f. If the officer can identify the suspect in order to obtain a warrant later.

#### B. Primary officer responsibilities

1. The officer's primary responsibility in a pursuit is the safe operation of the vehicle. Only marked vehicles with emergency equipment shall pursue.
2. Upon engaging in a pursuit, the pursuing vehicle shall activate appropriate warning equipment.
3. The officer shall notify the dispatcher of the following:
  - a. The location of the officer and the suspect's vehicle.
  - b. The direction of travel.
  - c. The license number (and state) of the suspect's vehicle.
  - d. The description of the suspect's vehicle.
  - e. The reason for the pursuit.
4. The officers will, to the best of their ability, keep the dispatcher informed of the location and direction of travel.
5. The officer will request the dispatcher notify a supervisor and Chief of Police when a pursuit is initiated.
6. Whenever the risk to the public or to the officer outweighs the immediate need to apprehend the suspect, the officer will terminate the pursuit.

#### C. Supervisor's responsibilities

1. The supervisor shall monitor the pursuit and has the responsibility to ensure that it is conducted in compliance with department policy. This includes directing officers to join or abandon pursuit, re-designating primary and support pursuing vehicles if necessary, approving or directing pursuit tactics, and terminating the pursuit.

2. The supervisor shall monitor the pursuit and may respond to the location of the stopped suspect. The supervisor may end the pursuit at any time that he or she feels circumstances warrant.
3. No more than two department vehicles may pursue a fleeing suspect without the specific authorization of a supervisor. In authorizing additional department vehicles to pursue, the supervisor shall consider:
  - a. The nature of the offense.
  - b. The number of suspects.
  - c. The number of officers currently participating as primary or support vehicles.
  - d. Any injuries or property damage already sustained as a result of the pursuit.
  - e. Any other clear, articulated facts that would justify the assignment of additional department vehicles.
4. After the incident, the supervisor shall critique the pursuit with all of the officers involved and direct participants to submit reports.
5. The supervisor at the time the pursuit was begun will retain authority over the pursuing officers of the department for the duration of the pursuit.
6. The supervisor may direct the use of tire-deflation devices, as appropriate. See paragraph J.12 below.

D. Supporting officers' responsibilities.

1. Normally the first back-up unit to respond shall help the primary officer in pursuing the suspect and making the arrest.
2. The secondary pursuing officer is responsible for broadcasting the progress of the pursuit and controlling the pursuit tactics. Without being tasked with these communications responsibilities, the primary officer can focus attention on the pursuit driving.

E. Rules of pursuits

1. Officers shall not intentionally ram, bump, or collide with a fleeing vehicle nor shall officers pull alongside such vehicles in an attempt to force them off the road or into an obstacle.
2. Boxing-in shall be performed only at low speeds and under the direct authorization of a supervisor and then only if the participating officers have been trained in the technique.

3. Caravanning is prohibited. Only two department vehicles (excluding the supervisor) shall participate in a pursuit at any time unless specifically authorized by a supervisor.
4. Officers shall not fire their weapons from a moving department vehicle.
5. If the on-duty supervisor orders the pursuit to end, the primary and supporting pursuing officers shall cease immediately. Also, the pursuing officer(s) shall end the pursuit if at any time during the course of the pursuit he or she loses sight of the fleeing vehicle for more than a few seconds.
6. The use of a stationary or rolling roadblock is prohibited. (TBP: 7.18)
7. When accompanied by civilian passengers, officers shall not pursue.
8. When two vehicles are involved in pursuit, each unit shall maintain a safe distance especially when passing through intersections. Each unit involved in the pursuit shall use a different siren-sound selection, if circumstances and safety permit. The use of different siren-sound combinations can help the primary and secondary vehicles hear one another and alert motorists and bystanders that two vehicles are operating under emergency conditions.
9. Should the suspect drive in a direction opposite to the flow of traffic, the pursuing officer shall not follow the suspect in the wrong direction but instead transmit via radio detailed observations about the suspect vehicle's location, speed, and direction of travel. The pursuing officer may be able to follow the suspect on a parallel road.
10. Officers involved in a pursuit shall not try to overtake or pass the suspect's vehicle.
11. Intersections are a particular source of danger. When approaching an intersection where signal lights or stop signs control the flow of traffic, officers shall:
  - a. Slow and enter the intersection at a reduced speed and only when safe, when all other vehicles are aware of the officer's presence.
  - b. Resume pursuit speed only when safe. When using emergency lights, siren, and headlamps, the officer is requesting the right of way and does not absolutely have the right to run a red traffic light or stop sign.
12. Tire Deflation Devices (TBP: 7.19)
  - a. Officers who have been trained in the use of tire deflation devices are authorized to deploy the devices when approved by a supervisor.

- b. Deployment must be made in safety and in an area that is free of obstructions for at least 100 yards in each direction.
- c. Deployment is made per manufacturer's instructions, always keeping the deploying officer safe from possible vehicular danger.
- d. The devices must be retracted prior to departmental vehicles running over them.
- e. Officers deploying the device will notify on-coming departmental vehicles of the deployment location so that they may slow down and avoid running over the devices.

F. Out-of-jurisdiction pursuits

- 1. Pursuits beyond the local jurisdiction require the direct approval of the supervisor and, if approved, shall be conducted according to this order. The dispatcher shall notify the appropriate jurisdiction of the pursuit and request help.
- 2. Once the pursuit has entered another jurisdiction, if officers from that jurisdiction enter the pursuit, department officers shall cease their emergency driving (unless circumstances require their continued pursuit, eg. Only one vehicle is involved in the pursuit), turn off emergency equipment, and follow the pursuit while observing all posted speed limits and traffic control devices.
- 3. If officers from another jurisdiction pursue a suspect into our jurisdiction, department officers shall enter the pursuit only if the other agency specifically requests help and the supervisor approves the participation. However, if the other agency has two or more officers pursuing a vehicle into our jurisdiction officers shall not enter the pursuit. Any non-pursuit assistance (including apprehension of a stopped suspect, securing intersections, etc.) may be provided as the circumstances dictate. Officers of this department shall not leave our jurisdiction to assist in a pursuit originating outside of our jurisdiction, unless approved by a supervisor and only if the other agency pursuing officer has no other backup to assist.
- 4. A fleeing suspect when arrested shall be taken before a judicial officer of the jurisdiction in which he/she was arrested regardless of where the pursuit began. The pursuing officers from the original jurisdiction shall then go before their local magistrate to obtain a warrant and ensure that a teletype is sent to the apprehending jurisdiction as soon as possible, acting as a detainer.




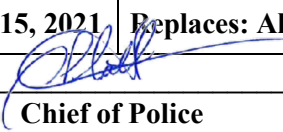
5. When a fleeing suspect from another jurisdiction is apprehended within the county, the apprehending officer shall take the arrested person before the appropriate magistrate. The on-duty supervisor shall confer with the other jurisdiction to determine which shall maintain custody of the suspect based upon the seriousness of the charges and the likelihood of release by respective magistrate.

#### G. TERMINATING PURSUITS

1. This order has noted the necessity for a pursuing officer to continuously evaluate the risks and goal of a pursuit. Under some conditions, abandoning a pursuit may prove the most intelligent decision the officer can make.
2. Officers shall discontinue a pursuit under the following circumstances:
  - a. The on-duty supervisor orders it.
  - b. The pursuing vehicle experiences an equipment or mechanical failure that renders the vehicle unsafe for emergency driving.
  - c. The pursued vehicle has outdistanced the pursuing officer such that its location is not known.
  - d. A person has been injured during the pursuit and no medical or department personnel are able to provide help.
  - e. The pursuing officer perceives a clear, unreasonable danger to officers, the fleeing suspect, or the public, and the danger created by continuing the pursuit outweighs the value of apprehending the suspect at the time.
  - f. The pursuing officer loses communications with the dispatchers.
3. Should the person(s) attempting to avoid apprehension stop the fleeing vehicle and precede on foot, the officer shall stop, give his or her location, and continue efforts to apprehend on foot. Circumstances may dictate, however, a continued pursuit in a vehicle. Support vehicles shall be dispatched in close proximity to offer assistance. The pursuing officer should be cautious, however, that the pursued vehicle may carry other persons who might assault the pursuing officers. Should the individual stop and remain in the vehicle, officers will not rush the vehicle. Appropriate felony stop procedures should be used.

## **V. FOLLOW-UP REQUIREMENTS (TBP: 7.14)**

- A. The supervisor shall ensure that all participating officers document their involvement in the pursuit whether or not the suspect was stopped. The initiating officer will complete a departmental Pursuit Report. Other officers involved will prepare a supplemental report documenting their participation. Reports shall be completed before the end of the officer's tour of duty.
- B. The supervisor shall collect and secure all video of the pursuit and shall review the pursuit for compliance with policy. The supervisor shall prepare a report, documenting their review of pursuit procedures with their findings and forward all documentation to the Chief of Police for review.
- C. The pursuit report with supervisory review will be forwarded to the Chief of Police. The Chief will also review the report and determine compliance with policy. The Chief of Police will inform the supervisor of his findings. Should a policy violation be identified, the Chief will direct that an investigation be conducted as necessary.
- D. Annually, the Chief of Police will cause an analysis of all vehicle pursuits occurring during the previous year to be conducted. The analysis will be designed to determine if the current policy is being followed, whether any changes are needed in the current policy, and any training needs of the department.

	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 7.16 Vehicle Impoundment and Inventory</b>
	<b>Effective Date: November 15, 2021   Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>
	<b>Reference:</b>

## I. POLICY

A motor vehicle is an important piece of personal property that must be properly managed and supervised if the police take it into custody. Because abandoned vehicles constitute a public nuisance and a hazard to traffic, members of our community view their removal as an essential police service. Also, vehicles involved in accidents or crimes may require towing and inventorying for evidentiary purposes. When towing is performed at an owner's request, the owner will be given the option of specifying a towing company. The department will select a tow company in other cases, typically by on call rotation. Officers will also specify a tow company if there is a traffic hazard and the tow company selected by an individual cannot arrive in a timely manner.

## II. PURPOSE

The purpose of this policy is to establish procedures for towing and for keeping an inventory of vehicles.

## III. AUTHORITY TO TOW

### A. Accident

1. Any vehicle involved in an accident shall be removed to the shoulder of the road or some other place out of the way of traffic as soon as possible after officers have obtained necessary investigative information.
2. Vehicles shall be removed from the shoulder without unnecessary delay.
3. The only departmental vehicles that can be used to push cars are ones that are equipped with push bars. The officer driving must have been trained in their use.
4. If the procedure above is not possible and a traffic hazard results, the officer may order towing of the vehicle at the owner's expense.

5. Vehicles may be impounded if the vehicle is needed for purposes of the investigation following a vehicle crash. Such cases may but do not necessarily involve custody of the operator.
6. Following vehicle crashes, an officer may request impoundment under one or more of the following circumstances:
  - a. The operator is unwilling or unable to take charge of the vehicle.
  - b. The vehicle cannot be legally parked and sufficiently secured at the scene.
  - c. There is property in or attached to the vehicle that cannot be sufficiently secured at the scene or placed in the custody of a responsible third party.

B. Emergency

Any vehicle found illegally parked in the vicinity of a fire, a traffic accident or an area of emergency that creates a traffic hazard or interferes with the necessary work of police, fire, or other rescue workers may be towed on an officer's orders at the owner's expense. Vehicles being used by radio, T.V., and press are exempt unless they obstruct police, fire, or rescue operations, or create an unreasonable traffic hazard.

Attempts to contact the owner to have them remove the vehicle should be made before calling a towing service.

C. Impeding/danger to traffic

No vehicle shall be stopped in such a manner as to impede or render dangerous the use of the highway by others except in cases of mechanical breakdown or accident. If a disabled vehicle is not promptly removed and creates a traffic hazard, the officer may order the vehicle towed at the owner's expense. [Local Ordinance Article 12.101(3)]

D. State/county/municipal vehicles

Paragraphs A, B, and C above shall not apply to any vehicle owned or controlled by the state or a local unit of government while engaged in construction or highway maintenance.

E. Blocking driveway or parking area

Any officer discovering or having report of any motor vehicle, or a trailer, or other vehicle blocking a driveway, or obstructing or interfering with the movement on any driveway without the landowner's permission may order the vehicle towed at the owner's expense. [Local Ordinance Article 12.101(5)]

F. Unattended traffic hazard/violation of law

Officers may call for the tow of any unattended motor vehicle found on a public street or grounds that constitutes a traffic hazard or is parked in such a manner as to be in violation of the law.

G. Unattended vehicle

Any motor vehicle left unattended upon any public roadway is subject to towing at the owner's expense. Officer's shall post a red tag notice, provided by the department, alerting the driver of the violation and intention to remove the vehicle. The vehicle shall not be removed until 48 hours after the notice has been posted.

H. Abandoned vehicle

1. Any motor vehicle abandoned on public property is subject to towing at the owner's expense.
2. A vehicle may be presumed to be abandoned if it lacks either a current license plate or has been left unattended on public property (other than an interstate or primary highway) for more than 48 hours.

I. Removal from private property

1. No removal shall be ordered, by members of this department, from any private property unless part of the process of abatement of junked vehicles pursuant City of Teague Ordinance 8.704.
2. Property or business owners may act immediately to have vehicles towed that are occupying a lot, area, space, building, or part thereof without permission of the owner.

J. Evidence/crime involvement

1. Upon supervisory approval, vehicles that are of an evidentiary value or have been used in the commission of a crime shall be towed at the request of the investigating officer to the City Yard (Magnolia Street), at department expense, where it can be safely secured.
2. Impoundment of stolen vehicles or those suspected of being stolen is appropriate under the following circumstances:
  - a. The owner cannot be contacted.
  - b. The owner is contacted and cannot or will not respond in a reasonable amount of time.

- c. Immediate removal is necessary for safety reasons or purposes of safekeeping.

**NOTE:** Towing of a vehicle that has been reported stolen is at the owner's expense.

**NOTE:** Officers should document reasonable efforts to contact owners with means readily available.

#### K. Prisoner's vehicles

1. Vehicles belonging to arrested persons that are left at the scene of the arrest may be at substantial risk of theft or of damage to the vehicle or to personal property contained in the vehicle. It is, therefore, the policy of this department to tow all prisoner's vehicles to an impound lot at the owner's expense for protection of the vehicle except in the following situations:
  - a. A friend or relative of the prisoner is at the scene, and the arrestee wishes to release the vehicle to that person provided the person possesses a current driver's license, and the arrestee consents to the release either in writing or on the audio/video in-car recording system.
  - b. The arrestee agrees to lock and leave the vehicle in a legal parking space where a parking violation will not occur before arrangements can be made to recover the car.
2. The officer may have the vehicle towed if he or she believes the above methods of vehicle release would not properly protect the vehicle or its contents.
3. A vehicle shall be towed if a subject is arrested and one of the following circumstances exists:
  - a. The vehicle was used in a crime.
  - b. The vehicle contains evidence of a crime that cannot be processed at the scene.
4. Officers should not unnecessarily impound motor vehicles for purposes of gathering evidence when such processing can be reasonably, effectively, and safely conducted at or near the scene.
5. A "hold" may be placed on any vehicle impounded for evidence for time necessary to complete evidence collection. Holds on vehicles must be approved by an agency supervisor to lessen financial impact on the city budget, as the department is responsible for these fees.
6. Investigating officers shall complete their investigation of the vehicle in a timely manner so that it can be released to the owner.

#### L. Impoundment for Forfeiture

1. As specified by state law, officers may impound a motor vehicle with the intent of initiating forfeiture proceedings when the vehicle is used in the commission of a crime.
2. Officers should contact a supervisor before initiating forfeiture proceedings and shall follow forfeiture procedures as provided by this agency.

### **IV. TOWING PROCEDURES**

- A. Motor vehicles shall not be impounded for purposes other than those defined by statute or ordinance. For example, vehicles cannot be impounded as a form of punishment, or as a means of conducting vehicle searches when probable cause does not exist or consent to search cannot be obtained.
- B. When an impoundment is ordered, the operator of the vehicle and any passengers should not be stranded. Officers shall take those measures necessary to ensure that the operator and any passengers of the vehicle are provided transportation.
- C. Vehicle operators may be permitted to remove unsecured valuables of a non-evidentiary nature from the vehicle prior to its removal for impoundment. The nature of these valuables shall be noted on the appropriate reporting document.
- D. Officers shall know under which provisions (subparagraphs A-J above) and laws the vehicle is to be towed.
- E. If the owner/operator does not wish to specify a towing firm or is not available to make a choice, the officer shall ask the dispatcher to send a rotation wrecker.
- F. In an emergency involving major traffic congestion owing to a disabled vehicle, the officer shall notify the dispatcher and request a rotation wrecker.
- G. If the vehicle involved in an emergency is larger than the normal passenger vehicle or pickup size, the officer shall so advise the dispatcher, who has a separate list of specially equipped wrecker services.
- H. When the wrecker arrives on the scene, the officer shall advise the dispatcher of time of arrival and any subsequent problems.
- I. Dispatchers shall be notified of all requests to tow vehicles by officers. Officers shall record date, time, place towed from and to, license number, make or model, and color of vehicle in the appropriate report.

- J. Contracted towing companies agree to respond to scenes within 20 minutes of a call. If a called wrecker does not arrive within the allotted time, the officer may ask the dispatcher to cancel the original wrecker and order a wrecker from another company.

## V. INVENTORY

### A. Authority and purpose:

1. A motor vehicle inventory is an administrative procedure designed to protect vehicles and their contents while in departmental custody.
2. The purpose of the inventory is to protect the owner's property and to protect the department against claims and possible dangers.
3. Inventories may be conducted without a warrant or probable cause in the following situations:
  - a. The vehicle has been lawfully seized or impounded.
  - b. Before towing the vehicle for violations, safety reasons, or other purposes as defined by law.


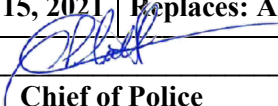
### B. Inventory vs. search

1. An examination of the contents of a motor vehicle pursuant to a criminal investigation or with the intent to search for evidence is not an inventory but a vehicle search and as such is governed by Policies 7.4 and 7.5.
2. Vehicles that are towed at the request of the owner/operator or vehicles that are left legally parked shall not be inventoried.
3. Officers are reminded of the "plain view doctrine" and the limitations upon the authority to search incidental to a lawful arrest. See Policy 7.4 for further details.
4. A vehicle inventory report shall be completed whenever an officer assumes responsibility for towing a vehicle and shall complete an inventory at the location where the vehicle was seized unless reasons of safety or practicality require the inventory to take place later or at a different location.
5. Before the vehicle is removed, officers shall obtain the signature of the tow-truck driver on the inventory report and provide the tow driver a duplicate copy of the report.
6. These inventories are further designed to protect the department from false claims of loss by others.



### C. Inventory procedures

1. The owner or operator of the vehicle shall be asked to remove, if possible, all valuables from the vehicle prior to impoundment. If such items cannot be removed, they shall be inventoried before the vehicle is removed.
2. The scope of the inventory includes all open and closed containers and compartments and any locked containers or compartments if the officer has a key. Locked or sealed areas shall not be forcibly entered if doing so will damage them. Locked areas that are not searched will be noted on the impound report. In general, the inventory extends to all areas of the vehicle in which personal property or hazardous materials may reasonably be found.
3. Officers shall not force open a vehicle's trunk or glove compartment to inventory the contents if a key is not available.
4. Any evidence, contraband, fruits of a crime, or instrumentalities of a crime discovered during an inventory shall be handled in accordance with evidence procedures.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.17 Communicable Diseases</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 8.10</b>	

**I. POLICY**

The department bears an obligation to the public and to its own personnel to increase awareness about risks, modes of transmission, and procedures for handling communicable diseases such as hepatitis B, tuberculosis, HIV (Human Immunodeficiency Virus) and AIDS (Acquired Immune Deficiency Syndrome), AIDS-related infections, along with COVID and COVID-Delta.

Officers cannot refuse to work with or handle anyone--victim, complainant, or suspect--because of the officer's fears of possible infection. Personnel shall not refuse to arrest or otherwise refuse to handle any person in a legitimate law-enforcement context, provided that appropriate protective equipment is available. The measures provided herein will assist officers in carrying out their duties while simultaneously minimizing health risks. Officers shall act responsibly in minimizing the risk of infection when dealing with any person, male or female, child, or adult, or with any body fluids. A few simple precautions, however, will avoid the risk of infection almost entirely.

The department shall provide employees with information and education on prevention of communicable diseases, as well as safety equipment and procedures to minimize their risks of exposure. The department has instituted post-exposure reporting, evaluation, and treatment for all members exposed to communicable diseases through the city safety protocols.

This policy is not intended to address all known diseases. For example, Ebola and other highly contagious diseases are not specifically addressed. Officers of this department will work closely with all stakeholders to develop response protocols that are safe and effective for everyone involved.

**II. PURPOSE**

The purpose of this order is to establish guidelines and procedures to be followed when a member of the department is exposed to a communicable disease with a risk of major illness or death, and for handling of evidence or property that may be contaminated.

### III. DEFINITIONS

#### A. Communicable disease

An infectious disease capable of being passed to another by contact with an infected person or his/her body fluids or on an object.

#### B. HIV (Human Immunodeficiency Virus)

The virus that causes AIDS. HIV infects and destroys certain white blood cells, undermining the body's ability to combat infection. (Also named HTLV-III or LAV). Technically speaking, this general order aims to reduce the chance of HIV transmission, the virus that causes AIDS. HIV is transmitted through very specific body fluids, including blood, semen, vaginal fluids, and breast milk.

#### C. ARC (AIDS-Related Complex)

A condition caused by the aids virus (HIV) and has a specific set of symptoms. Such symptoms include persistent fever, weight loss, skin rashes, diarrhea, and swollen lymph nodes. Although these symptoms may be debilitating, they are generally not life-threatening.

#### D. AIDS (Acquired Immune Deficiency Syndrome)

A blood borne and sexually transmitted disease that attacks and destroys the body's immune system. It makes people susceptible to infections, malignancies, and diseases not generally life-threatening to persons with normal immune systems. AIDS also causes disorders of the central nervous system. There is no vaccine against the virus. Personnel are advised that AIDS is not transmitted through any of the following (according to the Centers for Disease Control):

1. Sneezing, coughing, spitting.
2. Handshakes, hugging, or other nonsexual physical contact.
3. Toilet seats, bathtubs, or showers.
4. Various utensils, dishes, or linens used by persons with AIDS.
5. Articles worn or handled by persons with AIDS, i.e., doorknobs, pens, or cups.
6. Being near someone with AIDS frequently or over a long period of time.
7. Riding the same transportation.
8. Eating in the same public place with an AIDS-infected person.
9. Working in the same office.

#### E. Seropositivity

Refers to a person having antibodies to HIV, meaning that infection has occurred at some time in the past. A seropositive person can be infected with HIV for years without ever developing symptoms of AIDS. Infected persons can transmit the virus even though they may not have symptoms of AIDS.

#### F. Hepatitis B (HBV)

A viral infection that can result in jaundice, cirrhosis, and, sometimes, cancer of the liver. The virus is transmitted through exposure to blood, semen, vaginal secretions, breast milk, and possibly saliva. Two vaccines are currently available against hepatitis B [Recombivax (synthetic) or Heptivax (serum derived)].

#### G. Tuberculosis

A bacterial disease that can be transmitted through saliva, urine, blood, and other body fluids by persons infected with it. Tuberculosis is spread primarily through airborne droplets from infected coughing people. It can enter the body through infected mucous on the skin (as from coughing or sneezing) or from droplets that are inhaled. It is an airborne, opportunistic disease and it primarily causes lung infection. Although no vaccine against tuberculosis exists, medications are available to treat the disease.

#### H. Exposure control program

A written agency plan, available to all employees, which details the steps taken to eliminate or minimize exposure incidents and identifies at-risk tasks and assignments.

#### I. Personal protective equipment (PPE)

Specialized clothing or equipment worn or used by employees for protection against infection. PPE does not include uniforms or work clothes without special protective qualities.

#### J. Universal precautions

Controls or procedures advised by the Centers for Disease Control (CDC) that emphasize precautions based on the assumption that blood and body fluids are potentially infectious. This is true, for example, with persons thought to have been infected with the Ebola virus.

## K. COVID

Coronavirus disease (COVID-19) is an infectious disease caused by the SARS-CoV-2 virus.

Most people infected with the virus will experience mild to moderate respiratory illness and recover without requiring special treatment. However, some will become seriously ill and require medical attention. Older people and those with underlying medical conditions like cardiovascular disease, diabetes, chronic respiratory disease, or cancer are more likely to develop serious illness. Anyone can get sick with COVID-19 and become seriously ill or die at any age.

The virus can spread from an infected person's mouth or nose in small liquid particles when they cough, sneeze, speak, sing or breathe. These particles range from larger respiratory droplets to smaller aerosols.

### COVID – 19 Delta Variant

The Delta variant causes more infections and spreads faster than early forms of SARS-CoV-2, the virus that causes COVID-19. It has mutations in the gene encoding the SARS-CoV-2 spike protein, which are known to affect transmissibility of the virus as well as whether it can be neutralized by antibodies for previously circulating variants of the COVID-19 virus. It is thought to be one of the most transmissible respiratory viruses currently known. Symptomatology is similar to that of COVID-19.

## IV. GENERAL RESPONSIBILITIES

- A. The Chief of Police, or designee, shall ensure that adequate supplies are available for communicable disease control within the department. Supervisors are responsible for maintaining continuously an adequate supply of Personal Protective supplies for all affected personnel within their purview. Further, supervisors must ensure that:
  - 1. Personal protective equipment and supplies (PPE) can be found in sufficient quantities at advertised locations.
  - 2. Hypoallergenic gloves and other materials are available for employees allergic to standard-issue gear.
  - 3. Supplies are routinely inspected, replaced, cleaned.
  - 4. First Aid supplies and disinfectants are available always.
- B. The Chief of Police, through his or her subordinate supervisors, shall ensure that the department vehicles will contain the following PPE supplies:
  - 1. 3 pairs of disposable latex gloves

2. 1 disposable face mask
  3. 6 absorbent disposable towels
  4. 3 disposable plastic bags with contaminated material seals
  5. 1 bottle of alcohol-based cleanser
  6. 1 CPR shield (with a 1-way valve to prevent the patient's saliva from entering the caregiver's mouth)
  7. 1 pair of wrap-around safety goggles
  8. 1 carrying bag with zipper closure
  9. 1 pair disposable shoe coverings
  10. 2 puncture-resistant, leak proof containers for needles and other sharp objects
  11. 1 first aid kit
- C. Officers using supplies in their vehicles shall replace them or arrange to have them replaced as soon as possible. Officers shall always maintain disposable gloves in their personal possession.
- D. The Chief of Police or his designee shall cause to be maintained at the department office the following:
1. supply of disposable latex gloves
  2. orange/red plastic biohazard bags and tape, or plastic bags and sealing ties
  3. liquid household bleach
  4. disposable towels/towelettes
  5. buckets, mops
- E. Personnel shall use protective equipment under all appropriate circumstances unless the officer can justify otherwise.
- Officers who, for whatever reason, do not use protective gear when appropriate shall document the incident as soon as practicable for department review.
- F. All personnel whose skin contacts body fluids, of another, shall begin disinfection procedures immediately: these procedures range from simple soap-and-water washing to

the use of alcohol or antiseptic towelettes. All open cuts and abrasions shall be covered with waterproof bandages before personnel report for duty.

## **V. GENERAL PRECAUTIONS**

### **A. General**

Whenever possible, officers shall wear disposable latex gloves when doing any of the following:

1. Handling persons or items with any blood or body fluid products (hypodermic needles, syringes, or surfaces soiled with blood or body fluids, gun, or knife wounds).
2. Packaging and handling such items as evidence.
3. Cleaning up blood or other secretions which appear on floors, seats, equipment, handcuffs, shoes, clothing, pens, pencils, etc.

### **B. Specialized devices**

1. Masks shall be worn whenever splashes, spray, spatter, or droplets of potentially infectious fluids endanger contamination through the eyes, nose, or mouth. Masks may be worn with other protective devices such as goggles. Gowns, jackets, coats, aprons, or coveralls shall be worn as determined by the degree of exposure anticipated.
2. Fire Department personnel have access to complete bio-hazard suits and equipment if needed. (TEXAS BEST PRACTICES: 8.10)

### **C. Handling people**

1. Wash hands thoroughly for thirty seconds with warm water and soap after removing gloves (when handling evidence) or after contact with the subject (if bleeding or vomiting). If water is unavailable, use pre-moistened towelettes found in the communicable disease control kit to decontaminate skin.
2. Penetration resistant gloves or their equivalent should be worn when searching persons or dealing in environments, such as accident scenes, where sharp objects and bodily fluids may reasonably be encountered. Search techniques shall be used that require suspects to empty their own pockets or purses and remove sharp objects from their persons.
3. When transporting prisoners do not put fingers in or near any person's mouth.

4. Transport persons with body fluids on their persons in separate vehicles from other persons. A person who is bleeding or producing a fluid should be evaluated by Emergency Medical Services and bandaged before being transported.
5. Notify other support personnel or law-enforcement officers during a transfer of custody that the suspect has fluids on his or her person, or that the suspect has stated that he or she has a communicable disease. Booking forms should so state.

#### D. Handling objects

1. Objects contaminated with body fluids shall be completely dried, double bagged, in a brown paper bag, and marked to identify possible disease contamination.
2. Contaminated items to be disposed of shall be placed in Bio-Hazard bags and sealed.
3. Officers shall use extra care when handling any sharp objects. If officers find syringes, they shall not bend, recap, or otherwise manipulate the needle in any way, but shall place them in puncture-resistant containers provided by the department.

#### E. Handling fluids

1. Clean up blood spills or other body fluids with regular household bleach diluted 1-part bleach to 10 parts water (or use undiluted bleach, if easier). Bleach dilutions should be prepared at least every 24 hours to retain effectiveness.
2. Wear latex gloves during this procedure.
3. A soiled uniform (by blood or body fluids) should be changed as soon as possible. Wash in hot water and detergent or Dry Clean. If Dry Cleaning, advise the Dry Cleaner staff of the biohazard.
4. Departmental vehicles within which body fluids are spilled require immediate disinfection procedures. Employees who have the vehicles assigned to them shall notify their supervisor of the spill and arrange for a thorough cleaning as soon as possible.
5. All police vehicles will be cleaned with disinfectant as part of a routine, scheduled washing, and maintenance check.

#### F. Precautions when bitten

The danger of infection through bites is low. The victim cannot be infected with HIV through the blood of the biting person unless that person has blood in his or her mouth which contacts the victim's blood. HIV cannot be transmitted through saliva. With HBV, however, transmission takes place through infected blood or blood-derived body fluids. Infection takes place by exposure of the eyes, mouth, or mucous membranes to the virus. Precautionary procedures to minimize the risk of infection include:



1. Encouraging the wound to bleed by applying pressure and gently "milking" the wound.
2. Washing the area thoroughly with soap and hot running water.
3. Seeking medical attention at the nearest hospital (if the skin is broken).
4. Advising your supervisor, make a report, or follow any other policy for reporting injuries, including the filing of appropriate Worker's Compensation forms.

#### G. Precautions when punctured by needles or knives

If an officer is cut or punctured by a needle or a knife or other instrument while searching a suspect or handling contaminated evidence, follow these general guidelines:

1. Allow the wound to bleed (unless severe bleeding occurs) until all flow ceases. Then cleanse the wound with alcohol-based cleanser (or pre-moistened towelettes) and then with soap and water. Do not rely exclusively on towelettes: wash wounds thoroughly with soap and water.
2. Seek medical attention as soon as possible after the injury. A physician will then decide the proper treatment.
3. Advise your supervisor, make a report, or follow any other policy for reporting injuries, including the filing of appropriate Worker's Compensation forms.

#### H. Precautions at major crime scenes

1. At the crime scene, officers and crime scene technicians confront unusual hazards, especially when the crime scene involves violent behavior such as homicides where large amounts of blood have been shed.
  - a. No person at any crime scene shall eat, drink, or smoke due to the potential hazard.
  - b. The best protection is to wear disposable latex gloves. Any person with a cut, abrasion, or any other break in the skin on the hands should never handle blood or other body fluids without protection. Officers shall always carry latex gloves on their persons.
  - c. Latex gloves should be changed when they become torn or heavily soiled or if an officer leaves the crime scene (even temporarily).
  - d. If cotton gloves are worn when working with items having potential latent fingerprint value, wear cotton gloves over latex gloves.
  - e. Hands should be washed after gloves are removed, even if the gloves appear to be intact. Officers shall take care to avoid contact between skin and soiled gloves.

- f. Always keep a plastic bag in the communicable disease control kit to be used only to collect contaminated items (gloves, masks, etc.) until they can be disposed of properly. Clearly mark the bag "Contaminated Material."
  - g. Shoes and boots can become contaminated with blood. Wash with soap and water when leaving the crime scene or use protective disposable shoe coverings.
  - h. Wrap-around eye safety goggles or face masks should be worn when the possibility exists that dried or liquid particles of body fluids may strike the face. Particles of dried blood, when scraped, fly in many directions, so wear goggles and masks when removing the stain for laboratory analysis.
  - i. Crime scene search personnel will wear full coveralls, protective goggles, shoe covers, gloves, and particulate masks when entering a crime scene where large amounts of blood or other body fluids are expected.
2. While processing the crime scene, be constantly on the alert for sharp objects, such as hypodermic needles, razors, knives, broken glass, nails, etc. Use of mirrors may be appropriate while looking under car seats, beds, etc.
  3. Use tape--never metal staples--when packaging evidence.
  4. If practicable, use only disposable items at a crime scene where blood or other body fluids are present.
  5. Before releasing the crime scene, advise the owner of the potential infection risk and suggest that the owner contact the local health department for advice.
  6. Warning labels must be placed on all plastic evidence bags to go to the crime laboratory.

## **VI. OCCUPATIONAL EXPOSURE TO COMMUNICABLE DISEASES**

### **A. Notification**

1. As soon as practicable, all employees shall document possible exposure to infectious fluids or materials. In any case, employees shall immediately notify their supervisor of possible exposure.
2. Examples of such exposure include:
  - a. Direct contact with body fluids on chapped or open areas (cuts, scratches) on the skin or on mucous membranes (i.e., eyes, mouth).
  - b. Direct mouth-to-mouth resuscitation (CPR) without use of a one-way valve.

- c. Receiving a cut or puncture wound because of searching or arresting a suspect or handling contaminated evidence.

## B. Testing

1. If a member of the department is exposed to the body fluids of a person who has or is suspected to have a communicable disease, the member must be evaluated for evidence of infection by a physician.
  - a. The person whose body fluids contacts an officer may state that he or she has AIDS. Often, a person may try to prevent police from withdrawing blood for drug screening (as in a DWI arrest), although, in fact, he or she is not infected at all. While the department cannot coerce an individual--suspect or otherwise--to take periodic tests for infection, the department shall try to convince the subject who may have transmitted infection to do so.
  - b. HSC 81.050 states that if any person or employee has been exposed to body fluids, the person or employee whose fluids were involved will be requested by the agency to consent to HBV or HIV testing and disclosure of results.
  - c. CCP 21.31 provides measures whereby a person charged with any crime involving sexual assault, or offenses against children, may be ordered to submit to HIV testing.
  - d. Personnel should understand the difficulty of transmitting HIV and hepatitis B. If infection control measures have been followed, the risk is very low.

## C. Testing for presence of infection shall be done if indicated by a medical assessment (after an incident involving the possible transfer of blood or other body fluids). The following information details testing methods and their reliability.

### 1. AIDS/ARC/HIV

- a. Blood tests can detect HIV antibodies (produced by the body's immune system).
- b. The two common tests for HIV antibodies are the ELISA (Enzyme-Linked Immunosorbent Assay) and the Western Blot. Since the ELISA is less expensive and easier to perform, it is usually used as a first screen for HIV. If the ELISA identifies the person as seropositive, a second ELISA is performed. If the second test is also positive, a Western Blot is usually performed to confirm the results.
- c. Since HIV antibodies may not develop for some months after a person has been infected, an initial negative result may not mean freedom from infection. Typically, three to six months elapse following an infection for a positive reaction to occur. High false positive rates also occur with the use of only ELISA test.
- d. One must be tested, then, immediately following the incident (for a baseline) and then six and twelve months later.

## 2. Hepatitis B

A blood test can confirm the presence of hepatitis B virus six to eight weeks after exposure. Note that different tests exist for hepatitis B depending on the reason for testing.

## 3. Tuberculosis

This disease is detected first by a skin test, and then confirmed by an x-ray. A physician can order this test for the department employee.

### D. Confidentiality

1. Confidentiality of information concerning test results is paramount. The victim has a right to privacy in employer-maintained information about his/her health. No need exists for a supervisor routinely to know that a person tests positive (for HIV or hepatitis B). The department views a breach of confidentiality as a serious disciplinary problem which may result in suspension or termination of employment.
2. Under most circumstances, medical authorities will retain confidential records unless the employee tested requests it or state law requires it.

### E. Positive test results

1. Any person who tests positive for HIV or hepatitis B shall not be summarily removed from duty. The department shall make no restrictions simply because of diagnosis. These diseases are not spread by casual contact (as between coworkers in the department). The department shall alter an employee's assignment only when he or she can no longer perform the required duties.
2. The department shall ensure continued testing, if necessary, of members for evidence of infection, and shall provide psychological counseling if necessary.
3. Any person who tests positive for tuberculosis may be restricted from working. The medical evaluation will determine the stage and type of disease the person has contracted and if he/she is contagious. A tuberculosis-infected person requires medication and shall not return to work until the doctor says he/she is non-communicable. (Tuberculosis is easily transmitted. After exposure to tuberculosis, a person may, after a medical evaluation, take medicine to help prevent the disease.)

### F. Job performance

1. Infected employees shall continue working as long as they maintain acceptable performance and do not pose a safety or health threat to themselves or others in the department.

2. Where feasible, an employee who has medical complications from a communicable disease will either be reassigned to another job or have his/her job restructured so that he/she can remain employed. As necessary, medical documentation shall support requests for job restructure or reassignment. All personnel shall treat such employees in the same manner as employees who suffer from other serious diseases or handicaps: that is, fairly, courteously, and with dignity.

The department may require an employee to be examined by a physician to determine if he/she is able to perform his/her duties without hazard to him/herself or others.

#### G. Discrimination

The department expects all personnel to continue working relationships with any fellow employee recognized as having AIDS/ARC, hepatitis B, or non-communicable tuberculosis. The department will consider appropriate corrective or disciplinary action against an employee who threatens or refuses to work with an infected employee or who disrupts the department's mission.

#### H. Records

The agency maintains a record for each employee detailing incidents of occupational exposure, including information on vaccination status; the results of examinations and tests; health care professionals' written opinion; and any other relevant information. These records are retained by the Chief of Police and City Administrator in secure storage for the duration of tenure of employment and shall not be disclosed or reported without the express written consent of the employee.

### **VII. TRAINING**


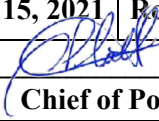
- A. The training officer shall ensure that all members of the agency receive a course of instruction on blood borne diseases and the use of Personal Protective equipment before their initial assignment. Further, each affected employee will receive annual refresher training plus any additional training appropriate to the employee assignment.
- B. The training officer shall retain complete records on instruction of employees to include dates of training; content of sessions; names and qualifications of trainers; names and job titles of attending employees.
- C. The training officer is responsible for dissemination of updated information to all personnel and for appropriate educational programs about communicable diseases. These programs shall include at a minimum:

1. Written information concerning AIDS/ARC/HIV, hepatitis B, and tuberculosis in the form of brochures, bulletins, memorandums, or fact sheets.
2. Group and/or individual presentations and discussions provided by adequately trained personnel or experts from outside the department.
3. Local resources for further medical and law-enforcement information.

### **VIII. AIDS-RELATED CONCERNS OF PERSONNEL**

ISSUE	INFORMATION
Human Bites	A person who bites is typically the one who gets the blood; viral transmission through saliva is highly unlikely. If bitten by anyone, gently milk wound to make it bleed, wash the area, and seek medical attention.
Spitting	Viral transmission through saliva is highly unlikely.
Urine/feces	Virus isolated in only very low concentrations in urine; not at all in feces; no cases of AIDS or HIV infection associated with either urine or feces.
CPR/first aid	To eliminate the already minimal risk associated with CPR, use masks/airways; avoid blood-to-blood contact by keeping open wounds covered and wearing gloves when in contact with bleeding wounds.
Body removal	Observe crime scene rule: do not touch anything; those who must contacts blood or other body fluids should wear gloves.
Casual contact	No cases of AIDS or HIV infection attributed to casual contact.
Any contact with blood or body fluids	Wash thoroughly with soap and water; clean up spills with 1:10 solution of household bleach.

\*Source: Adapted from: AIDS and the Law Enforcement Officer: Concerns and Policy Responses by Theodore M. Hammett, Ph.D., National Institute of Justice, U.S. Department of Justice, June 1987

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.20 Patrol Operations</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 7.01	

## I. POLICY

Patrol is the primary activity of law enforcement. It includes much more than driving through neighborhoods looking for evidence of lawbreaking. The department expects officers to conduct patrol vigorously to enforce traffic and criminal laws, answer complaints, conduct investigations, promote community-relations activities, and prevent crime.

## II. PURPOSE

The purpose of this policy is to define and outline general procedures for patrol operations. Procedures for handling specific calls for service are presented in the Patrol Standard Operating Procedures.

## III. ORGANIZATION AND ADMINISTRATION

### A. Organization

The patrol division is commanded by the Chief of Police and is comprised of officers assigned to both patrol and traffic functions under the direct supervision of sergeants. The sergeants report to the Chief of Police.

### B. Hours of Operation

The patrol division operates on a 24-hour, seven-days-a-week schedule. (TEXAS BEST PRACTICES: 7.01)

### C. Patrol Division Responsibilities

1. Responsible for the preliminary investigation of calls for police services, accident investigation, traffic enforcement, crime prevention, those duties which by their very nature require the actions of a police officer, and assignments which may be given by a commanding officer.
2. Composed of designated shifts, each under the command of a police sergeant or other designated supervisor who reports to the Chief of Police.

#### D. Personnel Staffing

1. Personnel are distributed among four patrol shifts. Personnel are assigned to a shift for a period of six months. The Chief of Police assigns personnel to shifts based upon distribution of calls for service and departmental staffing needs.
2. Minimum staffing for patrol functions is four sworn officers.
3. Personnel work (12) twelve-hour shifts, in an (84) eighty-hour pay period. This does not preclude the Chief of Police, based on the needs of the department or city, from changing the shift hours to a different type of assignment (e.g. 10 or 8 hour shifts, 80 hour pay period, etc.).
4. Personnel assigned to the patrol division are scheduled for rotating days off.

#### E. Assigned Personnel Levels by Shift

Current scheduling includes one-day shift officer, one-night shift officer, and a Sergeant on a swing shift (distributing their working hours between the two shifts).

### **IV. PROCEDURES - Conduct while on patrol**


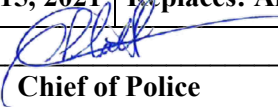
- A. Officers shall acquaint themselves with the geography of their patrol assignment, and particularly the location of highways and traffic hazards. Officers shall also become familiar with the names and addresses of habitual criminals and law violators, first-aid stations, hospitals, fire and rescue stations, magistrates, general district and county courts, medical examiners, public and private social service agencies, and any other public or private officials that prove helpful in the administration of their duties.
- B. Officers shall promptly respond to all calls dispatched to them. Calls that appear to be a risk to the physical well-being of a person take precedence over calls that are reporting danger or loss of property. In all cases, when dispatched to a call, the officer will respond directly and expediently.
- C. Officers shall initiate investigations into suspicious activities to prevent criminal activity.
- D. Officers shall monitor and enforce traffic laws and city ordinances as applicable. Officers are required, when stopping any motor vehicle for any reason, to document the stop for racial profiling purposes. Officers enforcing traffic laws shall issue a written warning or citation in every case. No verbal warnings are permitted as they cannot be properly tracked for racial profiling purposes.
- E. Patrol Officers are responsible for the preliminary investigations of criminal offenses occurring in the city.
- F. When an officer observes a violation of the law, subject to the authority and discretion discussed in Policy 1.2, he or she shall either (1) warn and release, (2) arrest, or (3) issue a summons to the violator to appear before the court having jurisdiction.



- G. Without exception, officers transporting non-department civilians (non-employees) shall notify the dispatcher of the transport. The report shall include the point of origin, vehicle odometer reading, and the destination. Upon arriving at the stated destination, the officer shall notify the dispatcher and give the odometer reading.
- H. To the capabilities of their training and qualifications, officers shall provide general and emergency assistance to motorists. Assistance includes providing information and directions, assisting stranded or disabled motorists, and obtaining medical and other emergency assistance. Officers shall, within reason, ensure that the requested service is provided in a timely fashion. If, after arranging for assistance, the officer is unable to remain with the motorists until help arrives, he/she shall take the necessary steps to provide safety to the motorists or arrange for transportation. If the need arises, officers may transport a motorist to a place of safety.

## **V. COMPLIANCE WITH PATROL STANDARD OPERATING PROCEDURE**

- A. The patrol Standard Operating Procedure manual is designed to provide direction to all officers in patrol operations and the handling of routine calls.
- B. All officers who respond to calls for service or calls to assist patrol officers will become familiar with the operational procedures. Officers are expected to follow the Patrol SOP unless specific other actions are approved or directed by a supervisor.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.30 Traffic Enforcement</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 7.21, 7.22, and 7.28	

## I. POLICY

Traffic law enforcement involves all activities or operations which relate to observing, detecting, and preventing traffic law violations and taking appropriate action under the circumstances. It is the policy of this department that motor vehicle stops shall be performed professionally and courteously, and with a view towards educating the public about proper driving procedures while recognizing and taking steps to minimize the dangers involved in this activity for the officer, the motorist, and other users of the highway.

Overzealous enforcement, however, without considering whether the violator is familiar with the legal requirements or without regard for the circumstances surrounding the violation causes disrespect for the law and poor relations between the department and the community. The emphasis of an officer's traffic enforcement is placed on violations that contribute to accidents and that prevent hazards to vehicular and pedestrian traffic. (TEXAS BEST PRACTICES: 7.28a)

## II. PURPOSE

It is the purpose of this policy to establish guidelines for stopping and approaching motorists in a manner that promotes the safety of the officer and the motorist.

## III. PROCEDURES

### A. Legal Basis for Stopping Motor Vehicles

1. Officers have legal justification for stopping a motor vehicle as provided by the Fourth Amendment to the U.S. Constitution. Without such justification, evidence of illegal activity discovered during a stop may be inadmissible in court.
2. Officers are prohibited from stopping vehicles under the guise of legal authority when in fact the stop is based solely on the officer's prejudice concerning a person's race, ethnicity, sex, or similar distinction.

3. A motor vehicle may be stopped only for a time that is reasonable to issue a citation or conduct other legitimate police business.
4. Officers should avoid arrests solely for minor vehicle infractions even if permitted by law when a citation in lieu of arrest is a reasonable alternative.
5. Officers are reminded that they have full discretionary authority in the type of enforcement actions to be taken, subject to the guidelines contained herein. Officers are encouraged to use good judgment, understanding, and compassion in deciding on the proper enforcement activity. (TEXAS BEST PRACTICES: 7.28b)

## B. Types of enforcement actions

### 1. Warnings

Officers may issue warnings to a violator whenever a minor traffic infraction is committed in areas where traffic accidents are minimal, or when the act may be due to ignorance of a local ordinance or other statutory law which may be a unique violation or a violation of which the driver may not be aware. In their discretion, officers must recognize that a properly administered warning can be more effective than any other type of enforcement.

### 2. Traffic Citation

A traffic citation shall be issued to a violator who jeopardizes the safe and efficient flow of vehicular and pedestrian traffic, including hazardous moving violations or operating unsafe and improperly equipped vehicles.

**NOTE:** A violator may not be physically arrested but must be issued a citation for the offenses of speeding or violation of the open container law.

### 3. Physical Arrest (TEXAS BEST PRACTICES: 7.28d)

- a. In compliance with Transportation Code 543.002, officers shall make a physical arrest and take the violator before a magistrate when the officer believes that the violator:
  - i. has committed a felony
  - ii. has failed to stop at the scene of an accident involving property damage or injury to another person or committed any other violation where the punishment is greater than a fine only

- iii. refuses to sign a written promise to appear under TRC 543.005 (Promise to Appear). In such cases, the officer shall contact a supervisor before an arrest is made. The supervisor shall go to the scene, contact the driver ensuring the violator understands the consequences for refusing to sign a promise to appear. The violator, if still refusing to sign the promise to appear, shall then be arrested and taken before a magistrate as required by statute.

#### C. Handling special categories of violators

##### 1. Juveniles

Juvenile traffic offenders are prosecuted in municipal court. Juveniles over the age of 14 may be issued citations for offenses committed in cars. Juveniles over the age of 10 may be issued citations for offenses on motorcycles, motorized scooters, or ATVs. Officers issuing traffic citations to juvenile offenders shall advise them that a parent or guardian must accompany them when they appear before the court. Juveniles must appear in court with their parents or other responsible adult. No prepayment is allowed.

##### 2. Foreign diplomatic or other consular officials

- a. Diplomatic immunity is granted by the United States Government. Generally, immunity may apply to diplomats, members of their families, and employees of diplomatic missions concerning acts performed in the course of their official duties.
- b. Different levels of immunity exist. The burden is on the diplomat to claim immunity and show the appropriate U.S. State Department-issued credentials.

##### 3. Members of Congress

- a. Members of Congress may not be detained for the issuance of a summons while they are in transit to or from the Congress of the United States.
- b. If a member of Congress is stopped for a traffic infraction, upon presentation of valid credentials, he or she shall be released immediately. The officer may then obtain a summons for the member of Congress covering the observed violation and make arrangements to serve the summons at a time when the member of Congress is not in transit to or from Congress or on official business.

#### D. Information regarding traffic summons

A citation shall be completed whenever a motorist is to be charged with a motor vehicle violation. Officers shall advise drivers of the following:

1. The court appearance schedule and contact information. (TEXAS BEST PRACTICES: 7.21)

2. Whether the court appearance by the motorist is mandatory
3. Whether the motorist may be allowed to pay the fine before court and enter a plea
4. Answers to the motorist's questions about the summons, being as thorough as possible.

#### **IV. UNIFORM ENFORCEMENT POLICIES FOR TRAFFIC LAW VIOLATIONS**

##### **A. Speed violations**

1. On public streets within the city that have a posted speed limit, officers shall not write citations for speeds less than 10 miles per hour over the posted or statutorily imposed speed limits, unless specifically approved for a particular operation or problem-solving activity or as directed by a supervisor.
2. In school zones, citations may be written for any vehicle traveling 5 miles per hour or greater over the posted school zone speed limit.

##### **B. Other hazardous violations**

Citations may be issued for any hazardous violation which in the officer's experience has caused accidents at the specific location.

##### **C. Equipment violations**

With only annual inspections required of vehicles, citations may be issued for any essential equipment defects which creates a danger or hazard to the driver or others. Officers are encouraged to use common sense when handling equipment violations. Officers should consider issuance of a warning but may revert to issuance of a citation if the driver has been previously warned and has not taken care of the violation.

##### **D. Public carrier/commercial vehicle violations**

In issuing a summons, consider traffic congestion, lack of parking, and carrier needs for delivery access. Repetitive violators shall be cited.

##### **E. Multiple violations**

Officers may issue citations for all appropriate violations. In the event of multiple violations, officers may issue multiple citations for the most serious violations and warn on others if appropriate.

F. Newly enacted laws

The law usually does not provide for a grace period when new laws take effect. Officers, though, may use discretion in observing a reasonable grace period before issuing a citation for the following:

1. A violation of a newly enacted traffic law.
2. Speeding violations in an area which the speed limit has been appropriately changed.
3. Expired state license tags for approximately ten days after their expiration.

**V. TRAFFIC LAW ENFORCEMENT PRACTICES - General**

Normal traffic enforcement involves patrol by officers who observe and handle traffic violations during the performance of their duties.

A. Area patrol involves traffic enforcement within the officer's assigned area of responsibility.

B. Line patrol involves traffic enforcement with concentration on a section of roadway.

C. Directed patrol instructions can specify enforcement in an area, on a line patrol, or at a specific location, depending on the nature of the hazard/violation.

D. Stationary observation, either covert or overt, may be used as a technique to make observations about the flow of traffic at a location.

E. Officers are encouraged, when completing reports or doing other activities which will keep them out of service for a short while, to park their patrol vehicles in a conspicuous location where the mere presence of the vehicle will serve to remind other drivers to comply with traffic laws.

F. Objectives of traffic stops

1. The two primary objectives of any traffic stop are

- a. to take proper and appropriate enforcement action; and
- b. to favorably alter the violator's future driving behavior.

2. Achievement of these objectives requires the officer to evaluate the violator's mental and physical condition when assessing the facts of the violation itself. In achieving these objectives, officers must exhibit flexibility to minimize conflict or argument with the violator.

G. Stopping a Violator / Issuing a Citation (TEXAS BEST PRACTICES: 7.28 c)

1. Rules to be followed in all traffic stops:
  - a. Be alert at all items for the unexpected.
  - b. Be certain that the observations of the traffic violation were accurate.
  - c. Present a professional image in dress, grooming, language, bearing, and emotional stability.
  - d. Be prepared for the contact by having the necessary equipment and forms immediately available.
2. Before making a vehicle stop:
  - a. Maintain a reasonable distance between the violator and the patrol vehicle.
  - b. Locate a safe spot to stop the vehicle.
  - c. Activate the emergency lights and, when necessary, the siren to signal the vehicle to stop.
  - d. Advise the dispatcher of the intention to stop the vehicle, and give the following information:
    - i. The location of the stop.
    - ii. The vehicle's license tag number and a description, to include the number of occupants, when necessary.
  - e. The officer shall position the patrol vehicle approximately one-half to one car length behind the violator's vehicle. The patrol vehicle shall be positioned so that it will offer the officer some protection from oncoming traffic. This position shall be two feet outside and to the left of the violator's vehicle.
3. Additionally, when stopping a vehicle in which the occupant(s) is deemed to present a hazard to the officer's safety, perform the following actions:
  - a. Request a backup unit and calculate the stop so that the backup unit is in the immediate area before making the stop.
  - b. Train the unit's auxiliary lights (spotlight) on the occupant(s) of the vehicle when applicable.

- c. When necessary use the vehicle's public address system to give instructions to the occupant(s) of the violator's vehicle.
4. Hazards
- a. On multi-lane roadways, the officer shall insure the safety of the violator during the lane changes by gradually changing from lane to lane with the violator until the right side of the roadway is reached.
  - b. Should the violator stop abruptly in the wrong lane or in another undesirable location, the officer shall direct him or her to move to a safer location. Officers shall use the public address system to instruct violators to move to a safer location. If the officer's oral directions and gestures are misunderstood, the officer shall quickly leave the patrol vehicle and instruct the violator.
  - c. At night, officers shall exercise caution in selecting an appropriate place for the traffic stop. Once the violator has stopped, to maximize officer safety, use the spotlight, and employ emergency bar lights and emergency flashers.
5. Approaching the violator (Left Side Approach)
- a. The following steps in stopping and approaching a traffic violator are intended to provide maximum safety for the officer, the violator, and other users of the roadway. Varying conditions regarding the engineering of traffic flow, the urgency to stop the violator (drinking driver), and the existing volume of traffic may require adjusting or altering the recommended procedure. Follow these procedures unless circumstances dictate another reasonable method.
  - b. After properly advising the dispatch of the traffic stop, location, and vehicle license number, the officer shall leave the patrol vehicle and be continuously alert for any suspicious movement or actions on the part of the violator or other occupants in the violator's vehicle.
  - c. The officer shall approach from the rear of the violator's car, examine its rear seat, and stop behind the trailing edge of the left front door. On busy roadways, officers should consider the option of approaching the vehicle from the passenger's side (right) for officer safety. This position shall be maintained if there are only occupants in the front seat of the vehicle. From this position, the officer can communicate with the violator, and at the same time keep all occupants of the vehicle in view.
  - d. In cases where the violator's car has occupants in both the front and rear seats, the officer shall approach to the trailing edge of the left front door, alert for any unusual actions on the part of the occupants and choosing a path so the door cannot be used as a weapon against the officer. From this position, the officer can communicate with the violator and keep all occupants in view.



- e. In traffic stops made by two-officer patrol vehicles, the passenger officer shall handle all radio communications, write all notes, and act as an observer and cover for his or her fellow officer.

6. Approaching the violator (Right Side Approach)

- a. The following steps in stopping and approaching a traffic violator are intended to provide maximum safety for the officer, the violator, and other users of the roadway. Varying conditions regarding the engineering of traffic flow, the urgency to stop the violator (drinking driver), and the existing volume of traffic may require adjusting or altering the recommended procedure. Follow these procedures unless circumstances dictate another reasonable method.
- b. After properly advising the dispatch of the traffic stop, location, and vehicle license number, the officer shall leave the patrol vehicle and be continuously alert for any suspicious movement or actions on the part of the violator or other occupants in the violator's vehicle.
- c. The officer shall approach from the rear of the violator's car on the right side of the vehicle opposite the active traffic lane, look into its rear seat, and stop behind the trailing edge of the right front door. This position shall be maintained if there are only occupants in the front seat of the vehicle. From this position, the officer can communicate with the violator, and at the same time keep all occupants of the vehicle in view.
- d. In cases where the violator's car has occupants in both the front and rear seats, the officer shall approach to the trailing edge of the right front door, alert for any unusual actions on the part of the occupants and choosing a path so the door cannot be used as a weapon against the officer. From this position, the officer can communicate with the violator and keep all occupants in view.
- e. In traffic stops made by two-officer patrol vehicles, the passenger officer shall handle all radio communications, write all notes, and act as an observer and cover for his or her fellow officer.

7. Communicating with the violator

In transacting business with the violator, the officer shall observe the following rules:

- a. Greet the violator courteously with an appropriate title.
- b. Ask for and accept only the violator's driver license and liability insurance. If the driver offers money, the officer shall refuse it and advise the driver of the illegality of the offer.

- c. If the driver has no driver's license, obtain another document of identification.
- d. Inform the violator what traffic law he or she has violated and the intended enforcement action (do not keep the violator in suspense).
- e. Allow the driver to discuss the violation. Do not argue, berate, belittle, or otherwise orally abuse the violator.
- f. Complete the forms required for the enforcement action.
- g. If the enforcement action requires a court appearance, make sure the violator knows where and when to appear. Explain any alternatives to the violator, but do not predict the actions of the court. Provide the violator with the court information sheet.
- h. Inform the violator of the departmental procedures for making compliments/complaints (printed at the bottom of every citation/warning form).

Be alert to any emotional stress exhibited by the driver. If stress is present, the instructions may have to be repeated or the violator may need to calm down before resuming driving.

#### 8. Conducting the transaction

- a. Return the violator's driver's license, registration, and a copy of the citation or warning, if given.
- b. Release the defendant after he or she signs the citation and receives a copy of the citation.
- c. Assist the violator in safely re-entering the traffic flow.
- d. Do not follow the violator.

## **VI. CITATION ACCOUNTABILITY**

### A. Citation Book Security (TEXAS BEST PRACTICES: 7.22)

- 1. Citation issuing information, records, and storage of citations is the responsibility of the municipal court. This department utilizes electronic citations, which are generated through our on-board computer systems in each patrol vehicle.

### B. Citation Accountability

- 1. Officers are directly accountable for each citation. Audit will now be performed quarterly, and all missing citations must be accounted for. Failure to be able to account for each citation issue may result in disciplinary action as appropriate.

2. Officers will document information about the stop in the “officer notes” section of the electronic citation software.
3. Officers who make errors on citations and chose not to issue a citation form will check it as “VOID,” in the electronic citation software menu, and submit a “Voided Citation Memo” through the chain of command to the Chief of Police. (a copy of the citation must be attached.) The Chief of Police will note “Approved” followed by their initials and forward the citation, with the attached “Voided Citation Memo” to municipal court.
4. Officers who discover errors after citations have been sent to municipal court must prepare a memorandum for Request for Dismissal, or a request that the violations be amended including any pertinent information regarding said changes and send the request through the chain of command the Chief of Police for approval and forwarding to court.

#### C. Voided Citations

Citations marked “Void” will be received by municipal court and entered a voided document system so that those citations will not show up as missing.

### VII. TRAFFIC RECORDS SYSTEM

#### A. The Sergeants are responsible for compiling the following traffic information:

1. Traffic accident data (to include location and accident causes)
2. Traffic complaints
3. Traffic engineering deficiencies

#### B. The Sergeants are also responsible for compiling traffic enforcement data to include:

1. Analysis of traffic accidents
2. Analysis of traffic enforcement activities
3. Implementation of Selective Enforcement techniques and procedures
4. Deployment of traffic enforcement personnel
5. Evaluation of selective enforcement activities.

**Note:** “Selective enforcement” refers to selecting location and type of offense to enforce in addressing a problem. It does not refer to the selection of specific individuals to receive enforcement action.

- C. Annually the Sergeants will prepare and distribute both traffic and patrol personnel the analysis of accident data and contributing factors. Any recommendations for enforcement and selective enforcement at high accident locations will be included.

## **VIII. DWI/DUI ENFORCEMENT PROCEDURES**

### **A. Laws**

It is unlawful for any person to drive or operate any motor vehicle, boat, or train while under the influence of alcohol or while under the influence of any drug of any nature which may affect their ability to safely operate such equipment.

### **B. Responsibilities**

Officers shall be alert for suspected DWI offenders. Officers shall use and document standardized roadside sobriety tests. Officers must carefully document the behavior of the DWI beginning with observations of driving. Once the violator has been stopped, the officer shall note the suspect's appearance, responses to stimuli, speech, admissions of drinking, or drug ingestion.

### **C. Breathalyzer**

1. The security, care, and maintenance of the breathalyzer and all physical evidence obtained from it are the responsibility of breathalyzer operators and supervisors.
2. The breathalyzer is located at the Freestone County Sheriff's Office.

### **D. Sobriety tests**

1. Officers shall administer a minimum of three field sobriety tests from the following list, which names the commonly administered tests.
  - a. Gaze nystagmus (only if properly certified).
  - b. Walk and turn.
  - c. One-leg stand.
  - d. Reciting of alphabet.
  - e. Ten count.
  - f. Finger to Nose.

- g. Officers may employ additional tests, but they must be performed in the same order and manner every time and must be acceptable by the county prosecutor's office for use in court cases.
- 2. At the officer's discretion, he/she shall be arrested for DWI and taken to the county jail.
- 3. If an officer suspects that the vehicle operator was driving under the influence of both alcohol and drugs, or drugs alone, he may require the operator to have a blood test performed in addition to testing for alcohol. Blood samples shall be analyzed Texas Department of Public Safety Crime Lab for evidence of alcohol and for various illegal, prescription, and over-the-counter drugs.
- 4. The officer shall make a full written report of the circumstances of the DWI arrest, formation of probable cause, and witnesses' observations.

E. Arrest

- 1. The arresting officer shall perform the following:
  - a. Advise the arrestee of the statutory warning as contained on the Texas Department of Public Safety Driver Improvement and Control (DIC) form 24 (DIC-24).
  - b. Request a sample of the arrestee's breath or blood for analysis to determine the level of alcohol or drugs the person may be under the influence. The person does NOT have the right to consult an attorney before determining if they will provide a specimen or not.
  - c. If the arrestee refuses the available test, confiscate their driver's license, and issue them a DIC-25 Notice of Suspension and Temporary Driving Permit.
  - d. The officer should follow the procedures outlined by the county attorney's office in obtaining a search warrant to obtain a blood specimen without the violator's consent. These instructions and forms for application for the search warrant are available on the officer share drive at this department.

F. Blood-test procedure

- 1. Take the arrested person to a physician, registered professional nurse, graduate laboratory technician, or other technician designated by law, who shall withdraw blood for the purpose of determining its alcoholic content and drugs.
- 2. The arresting officer shall utilize the DWI blood kit for collection of blood specimens for analysis in DWI cases. The DWI kit contains the necessary forms, instructions, and blood vials (with packaging materials) necessary for DWI blood cases. Officers should follow the instructions contained in these kits.

- a. The officer shall obtain the medical person's information for their report and documentation on the forms contained in the DWI blood kit.
- b. The arresting officer shall take possession of the two vials and seal them in two containers designed to hold them, which are included with the DWI blood kit.
- c. The arresting officer shall further perform the following:
  - i. Ensure all forms contained in the DWI blood kit are completed.
  - ii. Ensure the blood vial integrity seals are properly applied and the blood vials are secured in the provided containers.
  - iii. Seal the kit with the provided integrity seal.
  - iv. Mail the DWI blood kit to the appropriate Texas Department of Public Safety Crime Lab for analysis.

#### G. Breath analysis

1. Chemical analysis of a person's breath shall be performed by any person certified in the operation of breathalyzer machines.
2. The arresting officer shall obtain documentation, typically a printout from the breathalyzer machine, from the administering official. This should be included with their case report and submitted to the county attorney's office.

#### H. Accident investigation

If the DWI suspect has been involved in a traffic accident, officers shall also undertake the following:

1. Identify any witnesses who saw the suspect operating a motor vehicle.
2. Question the witness about the suspect's condition, actions, and statements immediately after the accident.
3. Establish a time lapse from the time of the accident to the time of arrest.
4. Question the witnesses and the suspect about what, if anything, the suspect ingested between the time of the accident and the officer's arrival.

## **IX. SPECIAL TRAFFIC PROBLEMS**

A. Identification and referral of driver recommended for reexamination to the Department of Public Safety (DPS). During routine traffic law enforcement activities officers frequently encounter persons whom they suspect of being incompetent, physically, or mentally disabled, or having other conditions that might prevent the person from exercising reasonable and ordinary care over a motor vehicle. In all such cases, in addition to whatever enforcement he or she may take, the officer shall notify DPS of these findings or suspicions, giving the violator's full name, date of birth, operator license number, and a brief description of the disability noted. A driver deficiency report may be used for this purpose.

### **B. Pedestrian and bicycle safety**

The Chief of Police shall review the traffic accident records at least annually to determine what enforcement actions are needed to provide a proactive pedestrian/bicycle safety enforcement program. The Chief may recommend officer enforcement measures including steps to:

1. Reduce or eliminate human environmental factors leading to accidents.
2. Reduce or eliminate the behavior, decisions, and events that lead to the accidents.

### **C. Off-road vehicles (including dirt bikes, motorized scooters, and ATVs)**

1. Accidents involving off-road vehicles that do not occur on a public highway do not require a traffic accident report. If the responding officer finds it convenient, he or she may complete an accident report and attach it to the offense report.
2. Any officer observing an unlicensed off-road vehicle on the highways that cannot be operated legally on public highways shall order it removed and enforce appropriate laws.
3. Officers shall enforce compliance with vehicle registration laws as they pertain to off-road vehicles.
4. Officers shall enforce laws, rules, and regulations concerning the operation of off-road vehicles on public-owned trails, parks, or property.

## **X. ESCORTS**

### **A. General rules**


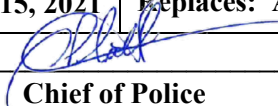
1. Officers shall not provide emergency or non-emergency escorts for private vehicles. If a medical emergency exists, then an ambulance should be summoned.

2. Officers may provide escorts of vehicles with oversize or hazardous loads. These escort duties shall be conducted under the authorization of the Chief of Police or a Sergeant. The Chief of Police or Sergeant shall coordinate the escort with the authority having control over the escorted vehicles. Further, the escort shall take place only per a written plan approved by the Chief of Police.
3. Officers may provide funeral escorts with marked vehicles

#### B. Funeral escorts

1. Before conducting a funeral escort, officers shall confer with the funeral home director to:
  - a. Plan the route to be taken to account for the most direct method, expected traffic density and anticipated obstacles.
  - b. Determine the circumstances of the escort to include which traffic lanes to use, speed of travel to the destination, and how to handle adverse weather.
2. Officers shall not lead funeral processions into an intersection on a red light. Once the procession has entered an intersection on a green light, the escorting officer shall take reasonable measures to allow the entire procession to continue even though the light changes.
3. No escorts shall be provided if the body of the deceased is not in the procession.



	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 7.31 Accident Investigations</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>
	<b>Reference:</b> Texas Best Practices 7.16

## I. POLICY

An objective of the department is the reduction of motor vehicle accidents. To accomplish this, the department performs a variety of functions such as providing emergency service to the injured, protecting the accident scene, conducting accident investigations and follow-ups, preparing reports, and taking proper enforcement action.

The purposes of accident investigation are to determine the causal factors of an automobile crash and use the information to develop enforcement that will reduce accidents. Accident reports are used by the Department of Public Safety and the Department of Transportation at the state level, and by the city locally to study the frequency of crashes at a given location and time, the causes of accidents, and the road conditions that existed when the accident occurred. The reports are also used to develop selective enforcement programs, to provide engineering studies, and to promote street and highway safety.

## II. PURPOSE

The purpose of this policy is to establish guidelines for the proper handling of traffic accidents and for the collection and use of data that will reduce automobile accidents resulting in property damage, injury, and death.

## III. PROCEDURES – General (TEXAS BEST PRACTICES: 7.16)

### A. Accident report and investigation, general

1. Texas Transportation Code requirements concerning the reporting of traffic accidents include the following:
  - a. TTC 550.001 Accidents and Accident Reports apply only to the following:
    - i. a road owned and controlled by a water control and improvement district; and

- ii. a private access way or parking area provided for a client or patron by a business, other than a private residential property, or the property of a garage or parking lot for which a charge is made for storing or parking a motor vehicle; and
    - iii. a highway or other public place.
  - b. TTC 550.026. The driver of any vehicle involved in an accident resulting in death or injury shall immediately notify law-enforcement officials.
  - c. TTC 550.062. A law-enforcement officer investigating an accident resulting in injury or death or total property damage to an apparent amount of \$1,000 or more shall make a written report of it to DPS. Officers who investigate an accident for which a report must be made, either at the time of and at the scene of the accident, or thereafter and elsewhere, by interviewing participants or witnesses, shall within 10 days after completing the investigation forward a written report of the accident.
- 2. An officer shall respond to and prepare a report of an accident involving any of the following:
  - a. Death or injury.
  - b. Property damage more than \$1,000.
  - c. Hit and run.
  - d. Impairment due to alcohol and/or drugs.
  - e. Hazardous materials.
- 3. Officers shall also be assigned to respond to the following:
  - a. Any accident involving disturbances between drivers or passengers.
  - b. Ones that create major traffic congestion.
  - c. Those in which vehicles are damaged to the extent that towing is required.
  - d. Patrol vehicles may be assigned to any other accident, not listed above, to assist persons involved with information exchange.
  - e. Time permitting, officers may investigate and report on accidents as supervisors direct.
  - f. Involvement of any city/county property, vehicles, equipment, facilities, or personnel

- g. Failure of either driver to produce a driver's license and proof of liability insurance

#### B. Responding to the accident scene

1. Officers shall respond to the scene of a minor accident code one unless a supervisor directs otherwise.
2. Officers shall respond code three to major accidents where there exist injuries or major road or highway blockages, or where information provided indicates the immediate need for an officer on scene.
3. The officers responding shall park their vehicles in a manner that will protect victims and the accident scene while still leaving room for other emergency service vehicles.

#### C. Accident scene responsibilities

1. The first officer to arrive at an accident scene shall perform the following:
  - a. Provide a scene "size up" to the dispatcher to alert other responding emergency services organizations for special needs or equipment.
  - b. Administer any needed emergency medical care (basic life support measures) pending arrival of rescue personnel.
  - c. Summon additional help as required (officers, EMS, fire department, wreckers).
  - d. Protect the accident scene.
  - e. Preserve short-lived evidence (broken parts, skid marks).
  - f. Establish a safe traffic pattern around the scene.
  - g. Locate witnesses.
  - h. Record key accident information.

Expedite removal of vehicles, persons, and debris from the roadway except for fatal accidents, in which case the scene is not to be disturbed.

2. The officer assigned to an accident shall have the responsibility and authority to request assistance from any other officers as needed. He or she becomes the primary investigating officer in charge at the scene unless the supervisor assumes this responsibility or determines that it is appropriate to assign these responsibilities to another officer.

3. Accident reports need not be filled out if the accident occurred on private property and the damage does not exceed \$1,000 unless the supervisor specifically asks for a report.
4. In case of extremely inclement weather where an accident involves only property damage, the officer may, with the supervisor's approval, perform the following:
  - a. Obtain information over the phone to complete the accident report and request that the involved drivers come to the department and file a report in person within 48 hours of the incident.
  - b. Complete a report showing the name, address, operator license number, and telephone number of each driver.

#### **IV. PROCEDURES - Accident scene**

##### **A. Collecting information**

1. At the scene of the accident, the investigating officer shall gather appropriate information for a report. Information to be collected at the scene may include, but is not limited to, the following:
  - a. Interview principals and witnesses and secure necessary identity/address/contact information.
  - b. Examine and record vehicle damage.
  - c. Examine and record the effects of the accident on the roadway or off the roadway on private or public property.
  - d. Take measurements as appropriate.
  - e. Take photographs as appropriate.
  - f. Collect and process evidence.
  - g. Make sure that the principals exchange information, such as insurance carriers, names, and phone numbers.

##### **B. Follow-up activities**

1. Follow-up activities that may be necessary include the following:
  - a. Obtain and record formal statements from witnesses.
  - b. Reconstruct the accident.
  - c. Submit evidentiary materials for laboratory examination.

- d. Prepare accident or offense reports to support charges arising from the accident.
2. In a particularly serious accident involving severe injuries, fatalities, or multiple vehicles, it may be necessary to summon expert or technical assistance from photographers, surveyors, mechanics, physicians, accident-crash team specialists, or other specialists. Expert assistance shall be requested through a supervisor.
3. Pursuant TTC 550.041 Officers are charged with investigating accidents and filing justifiable charges relating to the accident. To this end, the officer may take immediate enforcement action and issue a citation for observed violations or violations witnessed and supported by the investigative process. In death cases, the consultation with the county attorney may be necessary to decide the appropriate charge.
4. If the investigating officer concludes that the accident was caused by a person driving under the influence of intoxicants (DWI) and the defendant is still at the scene, the DWI arrest shall be made before transport.
5. If the driver is transported to the hospital before the officer arrives and if the officer later concludes that the driver was intoxicated, an arrest warrant shall be obtained. If the driver is hospitalized, the warrant will be served when the driver is released.
6. In other traffic-related investigations, when the officer leaves the scene of the offense and later identifies an offender or offense, arrest warrants may be obtained. The citation can be issued at the hospital after the accident scene has been processed.

#### C. Accident scene procedures

1. Upon notification of an accident, the officer assigned shall proceed promptly to the scene. If injuries have been reported, every effort should be made to avoid delay.
2. The patrol vehicle shall not be parked at the scene in a manner that will endanger pedestrians or motorists. The officer shall consider using the vehicle as a shield to protect the scene, those involved in the accident, and others working the scene, including the officer.
3. The officer shall leave the vehicle emergency lights on.
4. At all times when investigating an accident on the streets or highways, the officer shall wear a reflector safety vest.
5. Officers may use flares to create an illuminated warning pattern to alert other drivers. Note that flares may be dangerous at accidents where hazardous

materials are present. Caution and care should be taken when deploying the use of flares.

6. In case of fire danger from leaking or ruptured gas tanks or where the accident may involve hazardous materials, the on-scene officer shall summon the fire department.
  - a. All officers have been provided with a copy of the current emergency response guidebook to aid in identifying vehicles carrying hazardous materials. The guidebook illustrates hazardous materials placards and identifies and describes the relevant hazard, appropriate emergency procedures, and evacuation procedures.
  - b. Any officer arriving at the scene of such an accident who sees hazardous materials placards shall immediately summon the fire department. The fire department personnel will assume control of any scene involving hazardous materials and all officers shall provide support as required. The investigation of the accident shall begin after approval by the ranking fire department official on scene.
7. Any property belonging to accident victims shall be protected from theft or pilferage and, if owners are not present, it shall be taken into custody, tagged, and held for safekeeping until it is claimed by the owner.
8. Texas law requires any person clearing a wrecked or damaged vehicle from a highway to remove any glass or other injurious substances dropped upon the highway. Where the quantity of accident debris is too great for the wrecker operator to do this, the city public works services may be requested. The fire department shall assist in washing down combustible or caustic substances.
9. If either driver is not present at the accident scene, do not assume that it is a hit/run unless further inquiry indicates the possibility. Perform the following actions if the incident appears to be a hit/run.
  - a. As soon as practicable, transmit the description of the vehicle and driver to dispatch, along with the direction of travel and time elapsed since the incident.
  - b. Process the accident scene as a crime scene.

#### D. Accident report


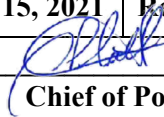
1. A report shall be filed on all accidents that occur on public property within the city if it meets any of the normal reporting criteria (death, personal injury, property damage in excess of \$1,000, or involvement of government-operated vehicles).

Public property is any highway, roadway, street, or public parking lot maintained by the state, county, or city.

2. In the event of an accident that occurs on private property, the individuals involved in the accident shall be informed to contact their insurance agencies to settle the claim. This department does not investigate private property accidents unless death or serious personal injury occurred or there is involvement of government-operated vehicles and that agency requests our agency investigate the matter.

E. Disabled vehicles

1. Officers shall not push or tow any vehicle with a patrol vehicle unless the patrol vehicle is equipped with a department-approved push bar and the officer has been trained in its use.
2. Owing to the risk to radio and emergency equipment, officers shall not connect jumper cables to a patrol vehicle to start a person's vehicle. Officers should summon a wrecker if a jump-start is required.
3. Officers shall direct motorists who are low on gas to the nearest station. If a vehicle is completely out of gas and no station in town is open, summon a wrecker on behalf of the motorist.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.40 Investigations</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 7.04, 7.05, 7.09 and 7.10	

**I. POLICY**

The primary purpose of an investigation is to collect facts leading to the identification and arrest of an offender and to organize and present the facts so that the result is a successful prosecution. The single most important criterion determining a successful investigation is the correct obtaining and handling of information supplied by an investigation of the crime scene, and from the victim(s) or witness(es) immediately after the crime.

The department expects officers to treat investigating as a skill developed through training and experience, a skill that demands intelligence, logic, and discipline.

Not every preliminary investigation will result in the identification of a suspect, an arrest, or the recovery of property. Solving a crime is most often a result of careful analysis of the physical evidence left at the scene or information provided by victims and witnesses. Follow up investigations are often necessary.

Because resources are limited, the department must prioritization their use. The department will investigate those crimes that are the most serious in nature and those that have the highest likelihood of solution.

**II. PURPOSE**

The purpose of this policy is to establish guidelines for the general conduct of preliminary and follow-up investigations.

**III. PROCEDURES: PRELIMINARY INVESTIGATIONS**

**A. General**

The preliminary investigation begins when the first officer arrives at the scene of a crime or when a citizen requests help, and it continues until an officer arrives and assumes responsibility. Patrol officers are responsible for the preliminary offense report in all cases except those specifically directed by a supervisor.



## B. Caution

Officers who first arrive at a possible crime scene must take care not to enter hastily. The crime scene may pose a threat to the officer: an armed suspect may still be at the scene, toxic chemicals or infectious materials may be present, or evidence may be destroyed if the officer enters. When practicable, officers shall first note the total environment of the scene including, for example, whether doors and windows are open or closed, lights on or off, presence of odors, and the condition and circumstances of the victim.

## C. After forming an impression of the entire scene and ensuring that no threat exists, the officer shall proceed with the preliminary investigation, which consists of, but is not limited to, the following activities:

1. Providing aid to the injured.
2. Defining the boundaries of and protecting the crime scene to ensure that evidence is not lost or contaminated. It should be cordoned with tape or rope. Any alterations to the crime scene should be recorded. Alterations might be caused by emergency assistance activity, the immediate necessity to handle evidence or assist victims, or the actions of witnesses or suspects at the scene.
3. Determining if an offense has been committed and, if so, the exact nature of the offense.
4. Determining the identity of the suspect or suspects and making an arrest if it can be accomplished either at the scene or through immediate pursuit.
5. Furnishing other officers with information concerning wanted suspects or vehicles including descriptions, method, and direction of flight or any other relevant information.
6. Determining the identity of all witnesses.
7. Collecting evidence officers will collect physical evidence to the limit of their ability and training. If the collection of evidence is beyond the capabilities or training of the officer, or is evidence in a serious crime, the officer shall contact a supervisor to determine available options for processing the crime scene, which may include contacting Texas Department of Public Safety Crime Scene Units.
8. Obtaining written statements from the victim, witnesses, and suspects.
9. Arranging for follow-up surveillance of the crime scene, if necessary.
10. Accurately and completely recording all pertinent information on the prescribed report forms.

## D. Follow-up

Officers will be responsible for conducting follow up investigations on cases they begin to work. Additional officers may assist in the investigative process if the initial officer is unable to do so because of shift assignment.

#### E. Supervisory responsibilities

1. Supervisors shall ensure that an adequate and complete preliminary investigation has been made, and shall review, screen, and approve the officer's preliminary report. Screening shall include a review of facts to ensure that all essential information is included and that the report is legible, clear, and complete. After the supervisor has reviewed, screened, and approved the report he/she will sign it.
2. Supervisors shall limit access to crime scenes to those persons immediately and directly connected with the investigation. Exceptions to this rule will not be made for other officers of the department, persons from other agencies, or members of the community, regardless of rank or position.
3. The supervisor shall authorize the call-out of a trained evidence technician, or other officers to assist, if necessary.
4. The supervisor may enlarge the preliminary crime scene, if necessary, by assigning officers to canvass the area for possible witnesses or suspects.

#### **IV. ASSIGNMENT OF FOLLOW-UP INVESTIGATIONS**

- A. All offenses shall be followed up by Officers primarily assigned to the case. Officers who conduct preliminary investigations of these offenses shall complete the original offense report with all details of the preliminary investigation included in the report.
- B. Responding officers who believe they cannot conduct a proper follow-up investigation (either because of lack of expertise, shift assignment, or any other reason) will contact their supervisor for direction.
- C. The supervisor shall provide guidance to officers conducting follow up investigations. The supervisor shall monitor the progress of all investigations to ensure they are being properly conducted with acceptable standards.

#### **V. PROCEDURES: FOLLOW-UP INVESTIGATIONS**

- A. Occasionally, additional investigation will be required at the end of the tour of duty of the assigned officer. In these cases, the supervisor shall determine whether the investigation should be (1) discontinued until the assigned officer's next tour of duty, (2) assigned to the next available officer, or (3) overtime should be authorized.
- B. Except where the investigation might be jeopardized by its temporary discontinuance, the original assigned officer shall handle the case.
- C. A supplemental report must be prepared by each officer who works on the case. A supplement recording the investigating officer's activity, the information developed, and case status shall be prepared and added to the original case file by the end of the investigating officer's shift. The officer shall maintain a case file to include the supplemental report.

- D. Officers conducting follow-up investigations shall continue the investigation of each criminal offense until it is brought to a conclusion or until there are no additional workable leads that would likely result in the identification of a suspect or recovery of property.
- E. If the officer's time is limited, follow-up of cases will be prioritized by seriousness of the crime and likelihood of identifying a suspect. Officers shall consult with their supervisors for additional assistance if cases with workable leads are not completed because of a shortage of personnel.
- F. Victims will be kept informed of the status of the case periodically and when the case is closed or suspended.
- G. Supervisors shall maintain a log of cases being worked by officers under their command. This log will be updated regularly when status supplements are received or when the case is closed or suspended. Officers and supervisors will keep the Chief of Police informed of the status of significant criminal cases.
- H. A follow-up investigation consists of, but is not limited to, the following activities:
  - 1. For most non-criminal cases:
    - a. Interviewing complainants and witnesses.
    - b. Locating missing persons.
    - c. Determining if information or suspicious activity relates to criminal activity.
    - d. Distributing information to the proper persons or agencies.
    - e. Locating lost property and returning same to the owner.
    - f. Investigating deaths, overdoses, suicides, and injuries to determine if a crime was committed.
    - g. Making necessary notifications or conducting necessary inspections.
    - h. Recording information.
  - 2. For most criminal cases:
    - a. Reviewing and analyzing reports of preliminary investigations.
    - b. Recording information.
    - c. Reviewing departmental records for investigative leads.
    - d. Seeking additional information from other officers, informants, contacts in the community, and other investigators/agencies or any other likely source.

- e. Interviewing victims and witnesses.
- f. Interrogating suspects.
- g. Monitoring social media sites of potential suspects, victims, and witnesses for information related to the case.
- h. Monitoring posted comments to on-line news stories about an offense.
- i. Arranging for the dissemination of information as appropriate.
- j. Planning, organizing, and conducting searches.
- k. Collecting physical evidence.
- l. Recovering stolen property.
- m. Arranging for the analysis and evaluation of evidence.
- n. Reviewing results from laboratory examinations.
- o. Identifying and apprehending the offender.
- p. Checking the suspect's criminal history.
- q. Consulting with the district attorney in preparing cases for court presentation and assisting in the prosecution.
- r. Notifying victims and witnesses when their presence is required in court.
- s. Testifying in court.
- t. Arranging for polygraph examinations, if necessary.

## **VI. REPORT WRITING**

### **A. Field notes.**

All formal reports begin with field notes. Field notes are important for the following reasons:

1. To create a permanent record of events.
2. To aid the investigation.
3. To ensure accurate testimony in court.
4. To protect the officer from false accusations.

B. Formal reports shall include the following information:

1. Date and time of arrival at the scene.
2. Relevant weather or situational conditions at the scene upon arrival (e.g., a fire, crowd).
3. Circumstances of how the crime was discovered and reported.
4. Identity of other officers or emergency personnel at the scene.
5. Physical evidence is present at the scene and the officers responsible for its collection.
6. Names, addresses, telephone numbers of victims or witnesses.
7. An accurate copying of field notes into the report.
8. Results of interviews with the complainant, victim, or witnesses to include the identity or description of suspects.
9. Diagrams, sketches, photographs, or video recording taken at the scene, and the identity of the photographer or artist.
10. Recommendations for further investigation.

## **VII. SOURCES OF INFORMATION**

A. Informants

Information is available from many sources, e.g., members of the community who wish to remain anonymous, criminals who have firsthand knowledge of illegal activity, and relatives or friends of those involved in crime. These sources shall be kept in mind when conducting investigations and interviews. Officers are cautioned to determine the motivation of people who provide information and closely evaluate it. For guidance on handling informants, consult Policy 7.43.

B. Interviews and interrogation

1. Field interviews

Field interviews are a productive tool and source of information for the department. They shall be used only in the pursuit of legitimate enforcement goals. When used properly they can discourage criminal activity, identify suspects, and add intelligence information to the files of known criminals.

2. Victim/witness interviews

- a. Officers must recognize the trauma/stress to which the victim or a witness has been subjected and shall conduct the interview in such a manner as to reduce stress.

- b. The age, physical limitations, and credibility of witnesses shall also be considered when evaluating their information.

### C. Interrogation of suspects

#### 1. Custodial statements and confessions.

- a. Miranda warnings are required and shall be administered prior to any custodial interrogation. Officers shall be familiar with the requirements in article 38.22 of the CCP and comply with these requirements.
- b. The following represent examples of situations that are not custodial and do not require issuance of Miranda warnings.
  - i. Investigatory stop and frisk or consensual encounters.
  - ii. Questioning during a routine traffic stop (or detention) or for a minor violation, which includes driving while intoxicated (DWI) stops until a custodial interrogation begins. During routine questioning at the scene of an incident or crime when the questions are not intended to elicit incriminating responses.
  - iii. During voluntary appearances at the police facility.
  - iv. When information or statements are made spontaneously, voluntarily, and without prompting by police. (Note: follow-up questions that exceed simple requests for clarification of initial statements may require Miranda warnings.)

#### 2. Administering Miranda.

- a. Miranda warnings shall be read by officers from the card containing this information to all persons subjected to custodial interrogation.
- b. Freelancing, recitation from memory, or paraphrasing the Miranda warnings is prohibited because it precludes officers from testifying in court as to the precise wording used.
- c. Officers shall ensure that suspects understand their right to remain silent and their right to an attorney. Suspects may be interrogated only when they have knowingly and intelligently waived their rights. Threats, false promises, or coercion to induce suspect statements is prohibited.
- d. The waiver of one or both Miranda rights must be performed affirmatively. Oral waivers are often sufficient but written waivers, particularly in felony charges, are preferred and should be obtained whenever possible on the appropriate agency form.

- e. Officers arresting deaf suspects shall notify their immediate supervisor and plan to procure the assistance of an interpreter in accordance with this agency's policy and state and federal law.
  - f. Officers arresting suspects who they believe may have limited English proficiency shall notify their immediate supervisor and plan to procure the assistance of an interpreter in accordance with this agency's policy and state and federal law.
3. Invoking the Right to Silence
- a. When a suspect invokes his/her right to remain silent, all interrogation shall terminate immediately.
  - b. Officers may interrogate a suspect who has previously invoked his right to silence if, after the passage of time, the suspect initiates communication with officers or fourteen (14) days have passed. However, prior to questioning Miranda warnings shall be re-administered and a waiver obtained.
4. Invoking the Right to Counsel
- a. If a suspect waives his/her right to counsel, a written waiver shall be obtained prior to questioning. If a suspect refers to counsel but his/her intentions are unclear, officers may question the suspect further to clarify his/her intentions. When a suspect invokes his/her right to counsel, all interrogation shall cease immediately.
  - b. The suspect may not again be interrogated about the crime for which he/she is charged, other crimes, or by other officers (from this or other agencies) unless (1) the suspect's attorney is present at the questioning; (2) there has been a break in custody of more than 14 days and the individual is re-advised of his Miranda rights and indicates he/she is waiving his right to counsel (written waiver), or (3) the suspect initiates new contact with the police. In this later case, Miranda rights must again be administered, and a waiver obtained before any questioning may take place. Officers shall also document and, if possible, obtain written verification that the suspect initiated the communication.
  - c. Officers shall cooperate in any reasonable way, after the suspect has asserted his rights, with efforts by counsel to contact or meet with suspects in custody.
5. Other Interrogation Requirements
- a. Parents or guardians shall be notified whenever a juvenile has been interrogated, taken into custody, or charged with an offense. Officers will take care when advising juveniles of their rights to ensure that the rights are understood before obtaining a waiver. Any juvenile statements obtained shall be done so in accordance with Texas Family Code Sections: 51.09 and 51.095.
  - b. The number of officers engaged in the interrogation shall be kept to a minimum.

- c. The interrogation shall be as short as possible.

#### D. Recording of Statements and Confessions

1. The circumstances surrounding the conduct of interrogations and recording of confessions shall be fully documented. This includes but is not necessarily limited to:
  - a. location, date, time of day, and duration of interrogation.
  - b. the identities of officers or others present.
  - c. Miranda warnings given, suspect responses, and waivers provided, if any; and
  - d. the nature and duration of breaks in questioning provided to the suspect for food, drink, use of lavatories or for other purposes.
2. Officers shall electronically record custodial interrogations conducted in a place of detention involving major crimes as defined by this department. Officers should record noncustodial interviews with suspects, witnesses, or victims during the initial interview phase of an investigation and may do so where deemed necessary, in accordance with law and departmental policy.
3. Electronic recording of juveniles shall be conducted if the juvenile suspect could be charged with a crime.
4. If electronic recordings cannot be conducted due to equipment failure, lack of suspect cooperation, or for any other reason deemed pertinent to successful interrogation by the officer, the basis for such occurrences shall be documented. This includes but is not limited to spontaneous declarations or other statements not elicited by police questioning.
5. Transporting officers need not refrain from questioning a suspect who has indicated a willingness to talk either at the scene or in route to the place of detention. However, officers shall not purposefully engage in custodial interrogations involving major crimes as defined by this policy to avoid this department's requirement for electronic recording.
6. Recording Protocol
  - a. Suspects do not have to be informed that they are being recorded unless required by law.
  - b. The office of the prosecutor, the investigative officer, or other authorized department official may direct that specific interrogations be recorded although they do not meet the criteria of major crimes as defined by departmental policy.



- c. The primary interrogator shall, where possible, obtain a signed waiver from the suspect before beginning interrogation. If the suspect elects not to be recorded or refuses to engage in the interrogation, the suspect's rejection shall be recorded. This does not preclude officials from continuing a recording of the events.
- d. Interrogations and confessions shall be recorded in their entirety, starting with the interrogator's entrance into the interview room and concluding with the departure of the interrogator and suspect.
- e. When commencing the recording, the primary interrogator shall ensure that voice identification is made of officers, suspect, and any others present, and that the date, time, and location of the interrogation is verbally recorded.
- f. When beginning a new recording, after a break, the interviewer shall announce the date and time the interrogation is being resumed.
- g. An authorized member of the department shall be assigned to monitor recording time to ensure the recording does not run out.
- h. Each recording shall include the following:
  - i. Declaration of the date, time, and place the recording began.
  - ii. Declaration of the start of the interrogation.
  - iii. Concurrence by the suspect that the interrogation has begun.
  - iv. Administration of Miranda warnings, even if the recording is a follow up to a prior interview or the suspect has been previously Mirandized.
  - v. Notation of the time the interrogation ends.
  - vi. Any lapse in the recording for comfort breaks or other reasons shall be accounted for on the recording. As an alternative, during a short recess, the recording may continue without interruption.
  - vii. Recording attorney-client conversations is prohibited.
  - viii. At the conclusion of the interrogations, the interrogator shall state that the interrogation is concluded and note the date of time or termination.
  - ix. The recording shall continue until all parties have left the interrogation room.
- i. Recordings of interviews are considered evidence and shall be handled as such. In addition, the following shall apply:
  - i. Unused recording media shall always be used for interrogations.

- ii. Both the original and copies of all recording media shall be protected from re-recording.
- iii. Only one interrogation shall be recorded on each recording tape, disk, or other material used in recording.
- iv. Before submitting the original recording to a secure evidence storage area, a copy of the recording shall be made. Copies shall be maintained in the case file and on the department computer server.
- v. The identifying information items supplied on the recording label shall be completed and the recording marked either as an original or a copy.
- vi. The reporting officer's follow-up report shall note if and how the interview was recorded.
- vii. All recordings shall be governed by this department's policy and procedures for the handling and preservation of evidence.

E. Collection, preservation, and use of physical evidence

- 1. Physical evidence is of major importance in all cases, particularly those without witnesses. The successful prosecution of a case often hinges on the quality of the physical evidence collected and preserved.
- 2. All officers are responsible for the preservation of evidence, and for maintaining and documenting the chain of custody of all evidence that is in their charge.

**VIII. CONSTITUTIONAL REQUIREMENTS: GENERAL**

- A. Officers conducting criminal investigations shall take all precautions necessary to ensure that all persons involved are afforded their constitutional protections. Officers shall ensure that:
  - 1. All statements, including confessions, are voluntary and non-coercive.
  - 2. All persons are advised of their rights in accordance with this general order.
  - 3. All arrested persons are taken promptly before a magistrate for formal charging.
  - 4. All persons accused or suspected of a criminal violation for which they are being interrogated are afforded an opportunity to consult with an attorney.
  - 5. Prejudicial pre-trial publicity of the accused is avoided so as not to interfere with a defendant's right to a fair and impartial trial.

**IX. RELATIONSHIP WITH COUNTY ATTORNEY**

- A. All personnel shall respond to requests for appointments from the county attorney, be on time, and be ready to discuss the subject at hand.

- B. In every contested case, misdemeanor or felony, the officer involved shall make an appointment with the county attorney or his/ her assistant to discuss the case before trial.
- C. During any investigation (or during planning for arrest or in pretrial stages), any questions of law or criminal procedure shall be addressed to the county attorney. Questions on law-enforcement procedures shall be addressed to the Chief of Police or supervisory staff.
- D. The county attorney may advise the Chief of Police of any cases where a decision was made not to prosecute or where the case was dismissed because of mishandling or error by an officer.

## **X. DISPOSITION OF CASES**

- A. The officer shall maintain files of all cases assigned to him/ her. All case files shall be appropriately labeled with the date of incident, the name of victim, and/or the name of any suspect or arrested person. Officers shall be aware of the requirement under state discovery laws in article 39.14 of the CCP that mandate virtually all writings and other items generated by the police during an investigation are subject to disclosure to the defense.


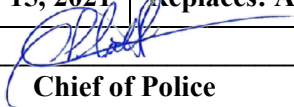
The file shall contain the following:

1. Original incident report and any supplementary reports or statements.
  2. Photographs.
  3. Lab reports,
  4. Reports of disposition of any property pertinent to the case, such that which was stolen, confiscated, recovered, or otherwise dealt with.
  5. Arrest reports
  6. Investigative notes
  7. All electronic and recorded communications – including but not limited to email, text, instant messages, and voice mail.
  8. All other items developed, documented, or seized during the investigation.
- B. When the investigation is complete, the investigator shall close the case under one of the labels listed below. A statement that explains the reasoning for the label shall be included in last paragraph of the report.
    1. Open. The case is still being actively investigated or worked on.
    2. Closed. The case has no further investigative leads or follow-up investigation to be conducted.

3. Cleared by Arrest. An arrest has been made in this case.
4. Exceptional Clearance. The identity and address or exact location of the culprit is known and sufficient evidence to obtain a warrant exists. However, due to some reason outside the control of the police, no arrest will be made. Examples: Complainant will not prosecute; district attorney will not prosecute; perpetrator is dead; subject arrested by another jurisdiction and no charges will be placed by the department.
5. False Report. The reporting party lied to mislead the police concerning the incident.
6. Unfounded. The offense did not actually occur in the first place, although at the time of the original report it was believed to have occurred. If the investigation has exhausted all leads, yet the possibility remains that new facts may come to light given future inquiry, the case shall remain open.

**NOTE:** Do not confuse “unfounded” and “false report.” It is a violation of the law to deliberately make a false report. An unfounded report is made in the belief that the offense occurred, but, in fact, it did not.

7. Inactive. All leads have been exhausted. No further investigation is possible or practical until new leads develop.
  8. Referred to Other Agency. The case has been referred to another agency for investigation or disposition.
- C. The officer’s supervisor shall approve the case closure in a manner consistent with current police reporting processes.
- D. When a case is closed, cleared by arrest, exceptionally cleared, or unfounded the case file is forwarded to the records custodian for filing.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.41 Crime Scene Processing</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 12.02	

## I. POLICY

Proper documentation, collection, preservation, and submission of physical evidence to forensic laboratories often provide the key to a successful investigation and prosecution. Through evidence located at the scene, a list of suspects might be developed, or suspects may be eliminated. Investigative leads can be established, and theories concerning the crime are substantiated or disproved. It is imperative, therefore, that each officer carefully process a crime scene, being sure not to overlook or contaminate or destroy evidence. Physical evidence appears in many shapes, sizes, and forms, thereby necessitating various recovery, preservation, and submission techniques. The investigating officer shall be prepared to collect, identify, and package the evidence so that it will not be changed in form and value when it reaches the laboratory. The officer collecting the evidence shall maintain a chain of custody of that evidence to ensure that it is presented to the court professionally and in compliance with the law.

## II. PURPOSE

The purpose of this policy is to establish responsibilities for officers who are investigating crime scenes and to establish guidelines for the proper documentation, collection, packaging, and submission of physical evidence to the forensic laboratory.

## III. DEFINITIONS

- A. Chain of custody: The chain of custody is the series of documented links between the time the evidence was obtained and the time it is presented in court. The links are documented by officers who handle the evidence, showing where and when they did so.
- B. Exclusionary rule: A rule of law that states that evidence seized or discovered in violation of the suspect's fourth, fifth, and sixth amendment rights cannot be admitted in court.
- C. Evidence: Any substance or material found or recovered in connection with a criminal investigation.

- D. Evidence custodian: The employee designated by the Chief of Police to have administrative oversight of all found or confiscated property that comes into departmental possession.

#### **IV. PROCEDURES. General crime scene processing**

- A. Depending on the nature of the crime and the type of evidence present, patrol officers will normally collect and submit physical evidence to the extent they have been trained and have the equipment to do so. Normally patrol officers will collect and submit evidence on misdemeanor and felony offenses where document or video evidence is the only physical evidence present.
- B. The department has several personnel trained and equipped to collect physical evidence. Patrol officers will contact a supervisor when the offense is a felony, any sex crime, child abuse, or where photographs are needed, or where the evidence present is beyond the capabilities of the officer's training or equipment.
- C. The officer who is called to a crime scene shall decide of the equipment needed for processing.
- D. The property and evidence form shall be used to document all property and evidence coming into custody of the department.
- E. Officers shall use the following general order of processing a crime scene unless reason dictates otherwise.
  - 1. Before moving objects or collecting evidence at crime scenes (except when it is necessary to help a victim, apply first aid, or handle a suspect), officers will photograph the scene. Photographs should start at the edge of the property and progress into the scene as needed to show the scene and its relationship to the evidence present. Close-up photographs of each piece of evidence will be taken with and without a measuring device in the picture.
  - 2. At major crime scenes, officers will also prepare a sketch of the scene. Sketches of any crime scene will be done if it will show relationships or locations of where evidence is collected.
  - 3. Before collecting any item of evidence, measurements using triangulation, or the coordinate method should be taken and recorded.
  - 4. Perishable evidence should be collected first. Perishable evidence -- such as fresh blood, blood-stained objects, physiological stains and tissue or biological material -- shall be collected and arranged to submit the material to a lab.

5. If the immediate destruction of evidence is not a concern, the officer should work through the scene systematically, collecting in a logical sequence and trying to avoid disrupting other items of evidence.
6. The officer should collect comparison samples, since the forensic laboratory can only compare known items with those showing similar characteristics. Sufficient specimens or controls must be submitted for comparisons of such items as hairs, fibers, paint, glass, soil, and tool marks.
7. Once perishable and other evidence has been collected, fingerprints shall be identified and lifted where possible. If transporting evidence may damage or destroy the latent prints on an object, the evidence shall be processed for prints at the scene.
8. Taking overall measurements -- that is wall, room, and building measurements -- is one of the last operations to be performed in processing the crime scene. The overall measurements are vital to produce the final crime-scene sketch but must be obtained last so as not to damage or destroy items of evidence.
9. One or more officers should conduct a final organized search in case evidence has been overlooked. If possible, the final search should be conducted by officers who have not participated in processing the scene.
10. The officer processing the crime scene shall enter each item collected on the evidence recovery log. The following information that should be recorded for each item:
  - a. A complete description of the item (including make, model, and serial numbers, if any).
  - b. The source (from whom and/or the location from which the item was obtained).
  - c. The name of the person collecting the item.
  - d. Date and time of collection.
  - e. Any transfer of collected items to another officer/person.
11. The officer processing a crime/incident scene shall prepare a report giving an accurate account of events. This information shall be placed in an offense/incident report.
12. All evidence shall be properly and prominently tagged or otherwise identified.
13. The recovering officer shall complete a chain-of-custody form for the property custodian.

14. Officers shall observe legal principles regarding the use of physical evidence. Officers shall rigorously maintain the chain of custody of all evidence and shall always remain mindful of constitutional safeguards. If officers are not scrupulous in observing these safeguards, the exclusionary rule may prohibit key evidence from being introduced at trial and the case may be lost or dismissed.

## **V. PROCEDURES. Evidence and property control**

### **A. Collection of evidence**

1. When collecting evidence, the officer shall use tongs or tweezers where possible. The officer shall avoid touching the evidence with his hands or anything that might contaminate the item.
2. Officers shall wear latex gloves while processing any crime scene. When collecting tissue or bodily fluid evidence, officers shall put on a new set of gloves after collecting each separate evidentiary item and discard the used gloves in a proper receptacle.
3. In collecting evidence, officers shall remain mindful about the possibility of contagion if the crime scene contains body fluids. Further, some evidence may consist of hazardous chemicals, waste products, explosives, or highly combustible materials. The evidence custodian in consultation with an evidence technician shall decide the best disposition of such items.
4. The officer shall unload weapons after he/she has examined the weapon in the exact condition it was found in, after photographs have been taken, and carefully marking how ammunition was loaded in the weapon.

### **B. Tagging evidence**

1. Officers will tag evidence in a manner consistent with their training and by following the guidance and recommendations of local prosecutorial staff.
2. Officers will document the items recovered at a crime scene both in the property section and the narrative section of the offense report.
3. Officers tagging evidence will use the current system established by the police department for the chain of custody and the actual evidence description.
4. Officers and other police personnel collecting and tagging evidence are expected to be able to readily testify in court regarding their exact involvement in the collection, tagging, and submission of all evidence seized.



### C. Packaging items of evidence

1. The officer who collects the evidence shall choose a container suitable for the type of evidence being packaged, and each piece of evidence should have its own container.
2. The exterior of the package should be labeled before the evidence is placed inside.
3. The officer should select a container that is appropriate for the size and weight of the item. He/she should give special consideration to moist or wet items, which could rot, rust, or otherwise deteriorate if packaged in plastic or an airtight container for an extended time.
4. The item should be packed in such a way as to minimize movement inside the container.

### D. Special circumstances

#### 1. Weapons

- a. No officer shall, under any circumstances, personally retain custody of any found or confiscated weapon.
- b. Officers bringing weapons into custody shall inspect them to ensure their safe storage. All firearms shall be unloaded before storage.
- c. The recovering officer shall check all confiscated or found weapons against NCIC/TCIC files.

#### 2. Drugs and narcotics. See Policy 12.1.

#### 3. Alcohol.

**NOTE:** The only alcoholic beverages that are considered contraband are those seized from underage persons whose possession is illegal.


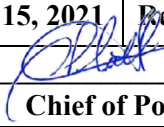
- a. All containers of alcoholic beverages shall be sealed or contained to avoid any chance of leakage.
- b. If not destroyed at the scene on video, the contraband alcoholic beverages shall be destroyed upon conclusion of legal proceedings, in a manner as prescribed by law.
- c. Alcoholic beverages seized or recovered that are not contraband or evidence shall be returned to the owner.

E. Preservation and submission of evidence to the forensic laboratory

1. Under normal circumstances, the officer who processed the crime scene is responsible for submitting evidence to the forensic laboratory.
2. Where more than one officer processed the scene, the supervisor shall choose an officer to take custody of all collected evidence and submit it to the laboratory for analysis.

F. Preservation of perishable or deteriorating items

1. When a rapidly deteriorating item of evidence has been collected (for example, a liquid sample of semen, a blood-soaked shirt), it shall be transported to the forensic laboratory the same day, if possible.
2. Any time an officer transports a perishable item to the laboratory for immediate analysis, the laboratory shall be called first so someone with authority to receive it will be available.
3. In cases where immediate transport to the forensic lab is not possible, it should be air dried for no more than one week and transported to the lab as soon as possible.
4. Where appropriate, submit known specimens of evidence so that comparisons can be made. The investigating officer shall be responsible for obtaining any required known specimens and submitting them, along with the items of evidence, to the forensic lab for analysis and comparison.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.42 Eyewitness Identification</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 7.32</b>	

## I. Purpose

The purpose of this policy is to outline proper protocol for eyewitness identification procedures for photographic, show-up, and live lineup identifications which maximize the reliability of identifications, protect innocent persons, and establish evidence that is reliable and conforms to established legal requirements.

## II. Policy

Eyewitness identifications are a significant component of many criminal investigations. The identification process must be carefully administered to minimize the likelihood of misidentifications. Moreover, constitutional safeguards must be observed in the process. The goal of reducing erroneous convictions can be furthered in many ways. Employing the most rigorous eyewitness identification methods is one way of doing this, but there are others. The eyewitness identification process is only one step in the criminal investigative process, albeit an important one. Corroborative evidence, for example, will lessen the impact of an erroneous eyewitness identification. The more other evidence that is available, the less risk there is of conviction based solely on erroneous eyewitness identification. There is no substitute for a competent and thorough criminal investigation.

This model policy was written to provide guidance on eyewitness identification procedures based on credible research on eyewitness memory and best practices designed not only to reduce erroneous eyewitness identification but also to enhance the reliability and objectivity of eyewitness identifications.

Evidence-based and best practices surrounding the collection and preservation of eyewitness evidence are addressed as are procedures to be employed where witnesses or victims are unable to read or write, are non-English speaking, or possess limited English language proficiency.

## III. Procedural Guidelines

### A. Definitions

1. **Blind Procedure** – A procedure wherein the person administering the live lineup or photo array does not know who the suspect is.
2. **Blinded Photo Array Procedure** – A procedure wherein the person who administers the photo array knows who the suspect is, but each photo is presented so that the administrator cannot see or track which photograph is being presented to the witness.
3. **Folder Shuffle Method** – A method of administering a photo array such that the administrator cannot see or track which photograph is being presented to the witness until after the procedure is completed. This method is employed when a blind procedure is not possible.
4. **Fillers** – Non-suspect photographs or persons. Fillers are selected to both fit the description of the perpetrator provided by the witness and to ensure that no individual or photo stands out.
5. **Illiterate Person** – An individual who speaks and understands English but cannot read and write in English.
6. **Interpreter** – An interpreter is a person who is fluent in English and the language of the witness or victim and who facilitates communication between two parties in two different languages. The term includes persons who facilitate communication with persons who are deaf, hearing impaired, or speaking impaired.
7. **Live lineup** – An identification procedure in which a group of persons is displayed to the witness or victim to identify or exclude the suspect.
8. **Person with Limited English Proficiency** – An individual who is unable to communicate effectively in English with a level of fluency that is typical of native English speakers. Such a person may have difficulty speaking, reading, or writing in English and includes persons who can comprehend English, but are physically unable to talk or write.
9. **Photo Array** – An identification procedure in which a series of photographs is displayed to the witness or victim to identify or exclude the suspect.
10. **Sequential Live Lineup or Photo Array** – An identification procedure in which the persons in the live lineup or the photographs in the photo array are displayed one by one (sequentially).
11. **Show-up** – An identification procedure in which a single suspect is shown to a victim or witness soon after the commission of a crime for the purpose of identifying or eliminating the suspect as the perpetrator.
12. **Witness Certification Statement** – A written statement that is read out loud to the witness or victim describing the procedures of the identification process.

## B. Selecting the Best Identification Method

1. Photo arrays are preferred over other techniques because: (a) they can be controlled better, (b) nervousness can be minimized, and (c) they are easier to manage logistically.
2. Because they involve multiple persons under relatively controlled circumstances, a properly conducted live lineup, like a properly conducted photo array, is preferable to a show-up.
3. Because they are highly suggestive, show-ups are vulnerable to challenges to their validity. Consequently, a show-up should be employed only where other indicia of guilt are present (e.g., suspect located relatively close in time and place to the crime).
4. Because witnesses may be influenced, however unintentionally, by cues from the person administering the procedure, a blind administrator should be used. This can be achieved using a blind procedure or a blinded photo array procedure (e.g. the folder shuffle method).
5. Because research shows the sequential presentation of live lineups and photo arrays is less likely to result in misidentification and carry very little risk of increasing the likelihood of failure to identify the suspect, a sequential presentation should be used.

## C. Selecting Fillers

All persons in the photo array or live lineup should be of the same sex and race and should be reasonably similar in age, height, weight, and general appearance. Ideally, the characteristics of the filler should be consistent with the description of the perpetrator provided by the witness(es). Where there is a limited or inadequate description of the perpetrator provided by the witness(es), where the description of the perpetrator differs significantly from the appearance of the suspect, where a witness has provided a highly detailed description, or where the witness's description of the perpetrator or the suspect has a highly distinctive feature, fillers should be chosen so that no person stands out in the live lineup or photo array.

## D. Explaining that the Perpetrator May or May Not Be Present

Because witnesses may be under pressure to identify a suspect, they should be informed that the suspect may or may not be present in a live lineup or photo array and that the person presented in a show-up may or may not be the perpetrator.

#### E. Explaining that the Investigation will Continue

The administrator should also explain to the witness that the investigation will continue, regardless of whether an identification is made, as another way of alleviating pressure on the witness to identify a suspect.

#### F. Witness Contamination

Precautions must be taken to ensure that witnesses do not encounter suspects or fillers at any time before or after the identification procedure. Avoid multiple identification procedures in which the same witness views the same suspect more than once. When showing a different suspect to the same witness, do not reuse the same fillers from a previous live lineup or photo array shown to that witness. Witnesses should not be allowed to confer with each other before, during, or after the identification procedure. Ensure that no one who knows the suspect's identity is present during live lineup or photo array procedure. In some live lineups, exceptions must be made to allow for the presence of defense counsel.

#### G. Documenting the Procedure

To strengthen the evidentiary value of the identification procedure, it should be documented in full. Video documentation is the preferred method. Audio recording is the preferred alternative. If neither method is employed, then the reason for not video or audio recording should be documented.

### **IV. Standard Operating Procedures**

The procedures which follow have been designed to: (a) reduce erroneous eyewitness identifications, (b) enhance the reliability and objectivity of eyewitness identifications, (c) collect and preserve eyewitness evidence properly, (d) respect the needs and wishes of victims and witnesses, and (d) address the needs of witnesses with limited English proficiency, where applicable.

To choose among the various identification methods, a brief description of each method follows in order of most preferred method to least preferred. Once the appropriate method is selected, the administrator should go directly to the Sample Standard Operating Procedures for that method. In any given situation only set of Sample Standard Operating Procedures applies.

#### A. Descriptions of Eyewitness Identification Methods

1. Sequential, Blind Photo Array – photo arrays where the photographs are presented one at a time to the witness or victim by a person who does not know who the suspect is. This method requires a preparer who may be familiar with the case and an administrator who does not know the identity of the suspect.

2. Sequential, Blinded Photo Array – photo arrays where the photographs are presented one at a time to the witness or victim by a person who knows who the suspect is, but who takes steps (putting the photographs in folders and shuffling them) to avoid knowledge of which person the witness or victim is looking at. This method typically involves an administrator who is familiar with the case and knows who the suspect is.
3. Sequential Live Lineup – live lineups where the persons in the live lineup are presented one at a time to the witness or victim. This method requires a preparer who may be familiar with the case and an administrator who does not know the identity of the suspect.
4. Show-up – procedure where the witness or victim is presented with a single suspect and asked to identify whether that suspect is the perpetrator. This procedure can be carried out by any officer.

## B. Standard Operating Procedures for Sequential, Blind Photo Array Administrations

### 1. Preparation

#### a. Designating a Preparer

Preparing the photo array should be undertaken by someone other than the person who will administer the photo array. Ideally, the investigating officer will prepare the photo array as this ensures that others who might be involved in the case are not used as fillers. Moreover, because the investigating officer knows who the suspect is, he or she should not be conducting the actual administration of the photo array.

#### b. Selecting Suspect Photograph

If multiple photos of the suspect are available, choose the photo that most resembles the suspect's appearance at the time of the crime. Do not include more than one photograph of the same suspect. If you do not know what the suspect looked like at the time of the crime, choose the photo that most resembles the victim's or witness's description of the perpetrator. If there are multiple suspects, include only one suspect's photo in the array.

#### c. Selecting Fillers

All persons in the photo array should be of the same sex and race and should be reasonably similar in age, height, weight, and general appearance. Ideally, the characteristics of the filler should be consistent with the description of the perpetrator provided by the witness(es). Where there is a limited or inadequate description of the perpetrator provided by the witness(es), where the description of the perpetrator differs significantly from the appearance of the suspect, fillers should be chosen so that no person stands out in the photo array. Do not mix color

and black and white photos. Use photos of the same size and basic composition. Never mix mug shots with other types of photographs.

d. Choosing Number of Fillers

Wherever possible, include a minimum of five fillers. Because increasing the number of fillers tends to increase the reliability of the procedure, one may have more than the minimum number of fillers.

e. Ensuring Similarity

Assess the array to ensure that no person stands out from the rest. Cover any portions of the photographs that provide identifying information on the suspect and similarly cover other photographs used in the array.

f. Placing Subject Photographs in Order

- i. Place a filler in the lead position.
- ii. Place the remaining photographs which will comprise the photo array in random order.
- iii. Place two blank photographs at the end (blanks on the same type of photographic paper as the actual photographs but which will not be shown to the witness; this is intended to cause the witness to think there may still be photographs to view in order to reduce pressure to choose what the witness may presume to be the last photograph).

g. Presenting the Photo Array to the Independent Administrator

Present the ordered photo array to the independent administrator. Do not tell the independent administrator which position the suspect is in.

2. Administration

The administrator of the photo array presentation should be an independent administrator who does not know the identity of the suspect and the witness should be informed of this. In a blind procedure, no one should be present who knows the suspect's identity.

a. Blinded Administration

If the blind procedure described above is not followed, then the photo array administrator should document the reason why and the administrator should be blinded. That is, he or she should conduct the photo array in a manner such that he or she does not know which person in the array the witness is looking at. There is a separate sample standard operating procedure for blinded photo array administration in this model policy immediately following this sample standard operating procedure.



b. Instruct Witness

Each witness should be instructed outside the presence of the other witnesses. The independent administrator should give the witness a written copy of the following Witness Certification Statement and should read the instruction statement aloud at the beginning of each identification procedure:

**In a moment, I am going to show you a series of photos. The person who committed the crime may or may not be included. I do not know whether the person being investigated is included.**

**Even if you identify someone during this procedure, I will continue to show you all photos in the series.**

**The investigation will continue whether or not you make an identification. Keep in mind that things like hair styles, beards, and mustaches can be easily changed and that complexion colors may look slightly different in photographs.**

**You should not feel you have to make an identification. It is as important to exclude innocent persons as it is to identify the perpetrator.**

**The photos will be shown to you one at a time. Take as much time as you need to look at each one. After each photo, I will ask you "Is this the person you saw [insert description of act here]?" Take your time answering the question. If you answer "Yes," I will then ask you, "In your own words, can you describe how certain you are?"**

**Because you are involved in an ongoing investigation, in order to prevent damaging the investigation, you should avoid discussing this identification procedure or its results.**

**Do you understand the way the photo array procedure will be conducted and the other instructions I have given you?**

c. Document Consent to Participate

Witnesses should then be asked to read the following additional paragraph and sign and date below.

**I have read these instructions, or they have been read to me, and I understand the instructions. I am prepared to review the photographs, and I will follow the instructions provided on this form.**

Some witnesses may decline to sign. When a witness declines to sign, it is sufficient for the investigating officer to document that the witness was appropriately instructed.

d. Presentation of Photographs

Present each photo to the witness separately (one at a time), in order. When the witness is finished viewing the photo, have the witness hand the photo back.

e. Question Witness

After the witness has looked at a photo and handed it back to you, ask: “**Is this the person you saw [insert description of act here]?**” If the witness answers “Yes,” ask the witness, “**In your own words, can you describe how certain you are?**”

f. Document Witness’s Responses

Document the witness’s response using the witness’s own words. Have the witness complete the appropriate section of the Witness Certification Statement to reflect the outcome of the procedure.

g. Show All Photographs

Even if the witness makes an identification, show the witness the next photo until you have gone through all the photographs. If a witness asks why he or she must view the rest of the photos, despite already making an identification, simply tell the witness that to assure objectivity and reliability, the witness is required to view all of the photographs.

h. Avoid Feedback During the Procedure

Do not give the witness any feedback regarding the individual selected or comment on the outcome of the identification procedure in any way. Be aware that witnesses may perceive such things as unintentional voice inflection or prolonged eye contact, in addition to off-hand words or phrases, as messages regarding their selection. Avoid casual conversation comments such as “very good.” Be polite but purposeful when you speak.

i. Additional Viewings

Only upon request of the witness, the witness may view the photo array again after the first photo array procedure has been completed. If the witness requests an additional viewing, the photo array administrator should present the entire photo array in the same order as the original presentation, a second time. If this occurs, it must be documented. The photo array administrator should never suggest an additional viewing to the witness. It is recommended that the witness not be allowed to view the photo array more than two times.

j. Subsequent Use of Materials

Ensure that if the witness writes on, marks, or in any way alters identification materials, those materials are not used in subsequent procedures.

- k. Multiple Identification Procedures with Same Witness

Avoid multiple identification procedures in which the same witness views the same suspect more than once.
  - l. Multiple Identification Procedures with Different Witness

If you need to show the same suspect to a new witness, have the preparer remix the photo array and renumber them accordingly.
  - m. Multiple Suspects

When there are multiple suspects, a separate photo array should be conducted for each suspect. There should not be more than one suspect per photo array.
  - n. Reuse of Fillers

When showing a different suspect to the same witness, do not reuse the same fillers from a previous array shown to that witness.
  - o. Contact Among Witnesses

To the extent possible, prevent witnesses from conferring with each other before, during, and after the photo array procedure.
  - p. Identification of Special Features

Only after an identification is made, a follow-up interview should assess any relevant factors that support the identification, such as: special facial features, hair, marks, etc.
3. Special Procedures are Required for Illiterate Persons or Persons Who Possess Limited English Proficiency
- a. Be Alert to People Who do not Speak English or Possess Limited English Proficiency

Given the diversity of communities, police officers may encounter persons who do not speak English or who possess limited English proficiency during a criminal investigation. When presented with this situation, officers should carefully consider the ethical and legal ramifications of how to handle the case when there is a language barrier.

b. Using an Interpreter

Unless the administrator speaks the victim's or witness's language fluently, an interpreter should be used for persons who do not speak English. The interpreter shall sign the Witness Instruction Statement on obtaining consent of a non-English speaking person to assist in the eyewitness identification process. Law enforcement personnel should consider arranging for an interpreter if a person interviewed:

- i. Is unable to communicate in English
- ii. Has a limited understanding of English
- iii. Is deaf, hearing impaired, or speaking impaired
- iv. Is otherwise physically challenged to communicate in English

c. Review and Explain Forms

If the person is unable to read, the administrator, in the presence of the witness, will give the explanation, read any forms, and obtain consent and acknowledge the consent on the Witness Certification Statement, stating why the person was unable to sign the form.

4. Documentation

To strengthen the evidentiary value of the administration it should be documented in full. Video documentation (with audio) is the preferred method. Audio recording is the preferred alternative. If neither method is employed, then the reason for not video or audio recording should be documented. Preserve the photo array, together with all information about the identification process.

C. Standard Operating Procedures for Sequential, Blinded Photo Array Administrations

1. Preparation

a. Select Suspect Photograph

If multiple photos of the suspect are available, choose the photo that most resembles the suspect's appearance at the time of the crime. Do not include more than one photograph of the same suspect. If you do not know what the suspect looked like at the time of the crime, choose the photo that most resembles the victim's or witness's description of the perpetrator. If there are multiple suspects, include only one suspect's photo in the array.

## b. Selecting Fillers

All persons in the photo array should be of the same sex and race and should be reasonably similar in age, height, weight, and general appearance. Ideally, the characteristics of the filler should be consistent with the description of the perpetrator provided by the witness(es). Where there is a limited or inadequate description of the perpetrator provided by the witness(es), where the description of the perpetrator differs significantly from the appearance of the suspect, fillers should be chosen so that no person stands out in the photo array. Do not mix color and black and white photos. Use photos of the same size and basic composition. Never mix mug shots with other types of photographs.

## c. Choosing Number of Fillers

Whenever possible, include a minimum of five fillers. Because increasing the number of fillers tends to increase the reliability of the procedure, one may have more than the minimum number of fillers.

## d. Ensuring Similarity

Assess the array to ensure that no person stands out from the rest. Cover any portions of the photographs that provide identifying information on the suspect and similarly cover other photographs used in the array.

## e. Placing Subject Photographs in Order

- i. Place a filler in a folder and set it aside for placement in the lead position.
- ii. Place the remaining photographs which will comprise the photo array in separate folders and place them in random order (mix them up) so you do not know which photograph is in which folder.
- iii. Take the folder you set aside in step 1), above and place it in the lead position.
- iv. Place two empty folders at the end.
- v. Number the folders.

## 2. Administration

### a. Blinded Administration

The purpose of a blinded administration is to conduct the photo array in a manner such that the administrator does not know which person in the array the witness is looking at.

b. Instruct Witness

Each witness should be instructed outside the presence of the other witnesses. The blinded administrator should give the witness a written copy of the following Witness Instruction Statement and should read the instruction statement aloud at the beginning of each identification procedure:

**The folders in front of you contain photos. In a moment, I am going to ask you to look at the photos. The person who committed the crime may or may not be included in the photos. I do not know whether the person being investigated is included.**

**Although I placed the photos into the folders, I have shuffled the folders so that right now I do not know which folder contains a particular photo.**

**Even if you identify someone during this procedure, I will continue to show you all photos in the series.**

**The investigation will continue whether or not you make an identification.**

**Keep in mind that things like hair styles, beards, and mustaches can be easily changed and that complexion colors may look slightly different in photographs.**

**You should not feel you have to make an identification. It is as important to exclude innocent persons as it is to identify the perpetrator.**

**You will look at the photos one at a time. When you open a folder, please open it in a manner that does not allow me to see the photo inside the folder. Take as much time as you need to look at each one.**

**When you have finished looking at a photo, close the folder and hand it to me. I will then ask you, "Is this the person you saw [insert description of act here]?" Take your time answering the question. If you answer "Yes," I will then ask you, "In your own words, can you describe how certain you are?"**

**Because you are involved in an ongoing investigation, in order to prevent compromising the investigation, you should avoid discussing this identification procedure or its results.**

**Do you understand the way the photo array procedure will be conducted and the other instructions I have given you?**

c. Document Consent to Participate

Witnesses should then be asked to read the following additional paragraph and sign and date below.

**I have read these instructions, or they have been read to me, and I understand the instructions. I am prepared to review the photographs, and I will follow the instructions provided on this form.**

Some witnesses may decline to sign. When a witness declines to sign, it is sufficient for the investigating officer to document that the witness was appropriately instructed.

d. Present Folders

Present each folder to the witness separately (one at a time), in order. The blinded administrator should not be able to view the photographs while the witness is viewing the photographs. The eyewitness should be the only person viewing the photographs. When the witness is finished viewing the photo, have the witness hand the folder back.

e. Question Witness

After the witness has looked at a photo and handed it back to you, ask: **“Is this the person you saw [insert description of act here]?”** If the witness answers "Yes," ask the witness, **“In your own words, can you describe how certain you are?”**

f. Document Witness’s Responses

Document the witness’s response using the witness’s own words. Have the witness complete the appropriate section of the Witness Certification Statement to reflect the outcome of the procedure.

g. Show All Folders with Photos

Show all folders containing photos to the witness. Even if the witness makes an identification, show the witness the next photo until you have gone through all the photographs. If a witness asks why he or she must view the rest of the photos, despite already making an identification, simply tell the witness that to assure objectivity and reliability, the witness is required to view all of the photographs.

h. Avoid Feedback During the Procedure

Do not give the witness any feedback regarding the individual selected or comment on the outcome of the identification procedure. Be aware that witnesses may perceive such things as unintentional voice inflection or prolonged eye contact, in addition to off-hand words or phrases, as messages regarding their selection. Avoid casual conversation comments such as “very good.” Be polite but purposeful when you speak.

i. Additional Viewings

Only upon request of the witness, the witness may view the photo array again after the first photo array procedure has been completed. If the witness requests an additional viewing, the photo array administrator should present the entire photo array in the same order as the original presentation, a second time. If this occurs, it must be documented. The photo array administrator should never suggest an additional viewing to the witness. It is recommended that the witness not be allowed to view the photo array more than two times.

j. Subsequent Use of Materials

Ensure that if the witness writes on, marks, or in any way alters identification materials, those materials are not used in subsequent procedures.

k. Multiple Identification Procedures with Same Witness

Avoid multiple identification procedures in which the same witness views the same suspect more than once.

l. Multiple Identification Procedures with Different Witness

If you need to show the same suspect to a new witness, remix the photo array as before and renumber them accordingly.

m. Multiple Suspects

When there are multiple suspects, a separate photo array should be conducted for each suspect. There should not be more than one suspect per photo array.

n. Reuse of Fillers

When showing a different suspect to the same witness, do not reuse the same fillers from a previous array shown to that witness.

o. Contact Among Witnesses

To the extent possible, prevent witnesses from conferring with each other before, during, and after the photo array procedure.

p. Identification of Special Features

Only after an identification is made, a follow-up interview should assess any relevant factors that support the identification, such as: special facial features, hair, marks, etc.

3. Special Procedures are Required for Illiterate Persons or Persons Who Possess Limited English Proficiency

a. Be Alert to People Who do not Speak English or Possess Limited English Proficiency

Given the diversity of communities, police officers may encounter persons who do not speak English or who possess limited English proficiency during a criminal investigation. Where presented with this situation, officers should carefully consider the ethical and legal ramifications of how to handle the case when there is a language barrier.



b. Using an Interpreter

Unless the administrator speaks the victim's or witness's language fluently, an interpreter should be used for persons who do not speak English. The interpreter shall sign the Witness Certification Statement on obtaining consent of a non-English speaking person to assist in the eyewitness identification process. Law enforcement personnel should consider arranging for an interpreter if a person interviewed:

- i. Is unable to communicate in English
- ii. Has a limited understanding of English
- iii. Is deaf, hearing impaired, or speaking impaired
- iv. Is otherwise physically challenged to communicate in English

c. Review and Explain Forms

If the person is unable to read, the administrator, in the presence of the witness, will give the explanation, read any forms, and obtain consent and acknowledge the consent on the Witness Instruction Statement, stating why the person was unable to sign the form.

4. Documentation

To strengthen the evidentiary value of the administration it should be documented in full. Video documentation (with audio) is the preferred method. Audio recording is the preferred alternative. If neither method is employed, then the reason for not video or audio recording should be documented. Preserve the photo array, together with all information about the identification process.

D. Standard Operating Procedures for Sequential, Blind Live lineups

1. Preparation

a. Designating a Preparer

Preparing the live lineup should be undertaken by someone other than the person who will administer the live lineup. Ideally, the investigating officer will prepare the live lineup as this ensures that others who might be involved in the case are not used as fillers. Moreover, because the investigating officer knows who the suspect is, he or she should not conduct the actual administration of the live lineup

b. Selecting Fillers

All persons in the live lineup should be of the same sex and race and should be reasonably similar in age, height, weight, and general appearance. Ideally, the characteristics of the filler should be consistent with the description of the perpetrator provided by the witness(es). Where there is a limited or inadequate

description of the perpetrator provided by the witness(es), where the description of the perpetrator differs significantly from the appearance of the suspect, fillers should be chosen so that no person stands out in the live lineup.

c. Choosing Number of Fillers

Whenever possible, include a minimum of five fillers. Because increasing the number of fillers tends to increase the reliability of the procedure, one may have more than the minimum number of fillers.

d. Ensuring Similarity

Assess the lineup to ensure that no person stands out from the rest.

e. Placing the Subjects in Order

Place a filler in the lead position and place the remaining persons who will comprise the live lineup in random order.

f. Presenting the Live lineup to Administrator

Present the ordered live lineup to the administrator. Do not tell the administrator which position the suspect is in.

2. Administration

The administrator of the live lineup should be an independent administrator who does not know the identity of the suspect and the witness should be informed of this. In a blind procedure, no one should be present who knows the suspect's identity. In some live lineups, exceptions must be made to allow for the presence of defense counsel. Once the live lineup commences, defense counsel's role is limited to that of observer.

a. Instruct Witness

Each witness should be instructed outside the presence of the other witnesses. The live lineup administrator should give the witness a written copy of the following Witness Certification Statement and should read the instruction statement aloud at the beginning of each identification procedure:

**In a moment, I am going to show you a series of individuals. The person who committed the crime may or may not be included. I do not know whether the person being investigated is included.**

**The investigation will continue whether or not you make an identification.**

**Even if you identify someone during this procedure, I will continue to show you all individuals in the series.**

**Keep in mind that things like hair styles, beards, and mustaches can be easily changed.**

**You should not feel you have to make an identification. It is as important to exclude innocent persons as it is to identify the perpetrator.**

**The individuals will be shown to you one at a time. Take as much time as you need to look at each one. After each individual, I will ask you "Is this the person you saw [Insert description of act]?" Take your time answering the question. If you answer "Yes," I will then ask you, "In your own words, can you describe how certain you are?"**

**Because you are involved in an ongoing investigation, in order to prevent damaging the investigation, you should avoid discussing this identification procedure or its results.**

**Do you understand the way the lineup procedure will be conducted and the other instructions I have given you?**

b. Document Consent to Participate

Witnesses should then be asked to read the following additional paragraph and sign and date below.

**I have read these instructions, or they have been read to me, and I understand the instructions. I am prepared to view the individuals who will be presented to me, and I will follow the instructions provided on this form.**

Some witnesses may decline to sign. When a witness declines to sign, it is sufficient for the investigating officer to document that the witness was appropriately instructed.

c. Presentation of Subjects

Begin with all live lineup participants out of the view of the witness. Present each subject one at a time in the order presented to the administrator by the preparer. Present everyone to the witness separately, removing those previously shown from the field of view.

d. Question Witness

After everyone is shown, ask the witness: **"Is this the person you saw [insert description of act]?"** If the witness answers "Yes," ask the witness, **"In your own words, can you describe how certain you are?"** Document the witness's response using the witness's own words.

e. Document Witness's Responses

Document the witness's response using the witness's own words. Have the witness complete the appropriate section of the Witness Certification Statement to reflect the outcome of the procedure.

f. Show Every Subject

Even if the witness makes an identification, show the witness the next subject until all subjects have been shown. If a witness asks why he or she must view the rest of the subjects despite already making an identification, simply tell the witness that to assure objectivity and reliability, the witness is required to view all of the subjects.

g. Consistency of Actions

Ensure that any identification actions (e.g., speaking, moving) are performed by all members of the live lineup.

h. Avoid Feedback During the Procedure

Do not give the witness any feedback regarding the individual selected or comment on the outcome of the identification procedure in any way. Be aware that witnesses may perceive such things as unintentional voice inflection or prolonged eye contact, in addition to off-hand words or phrases, as messages regarding their selection. Avoid casual comments such as "very good." Be polite but purposeful when you speak.

i. Additional Viewings

Only upon request of the witness, the witness may view the lineup again after the first live lineup has been completed. If the witness requests an additional viewing, the independent administrator should present the entire live lineup a second time. If this occurs, it must be documented. The live lineup administrator should never suggest additional viewing. It is recommended that the witness not be allowed to view the live lineup more than two times.

j. Multiple Identification Procedures with Same Witness

Avoid multiple identification procedures in which the same witness views the same suspect more than once.

k. Multiple Identification Procedures with Different Witness

If you need to show the same suspect to a new witness, have the preparer change the order of the subjects in the lineup.

l. Multiple Suspects

When there are multiple suspects, a separate live lineup should be conducted for each suspect. There should not be more than one suspect per lineup.

m. Reuse of Fillers

When showing a different suspect to the same witness, do not reuse the same fillers from a previous lineup shown to that witness.

n. Contact Among Witnesses

To the extent possible, prevent witnesses from conferring with each other before, during, and after the live lineup procedure.

o. Contact between Witnesses, Suspects, and Fillers

Take precautions to ensure that witnesses do not encounter suspects or fillers at any time before or after the identification procedure.

p. Identification of Special Features

Only after an identification is made, a follow-up interview should assess any relevant factors that support the identification, such as: special facial features, hair, marks, etc.

3. Special Procedures are Required for Illiterate Persons or Persons Who Possess Limited English Proficiency

a. Be Alert to People Who do not Speak English or Possess Limited English Proficiency

Given the diversity of communities, police officers may encounter persons who do not speak English or who possess limited English proficiency during a criminal investigation. Where presented with this situation, officers should carefully consider the ethical and legal ramifications of how to handle the case when there is a language barrier.

b. Using an Interpreter

Unless the administrator speaks the victim's or witness's language fluently, an interpreter should be used for persons who do not speak English. The interpreter shall sign the Witness Certification Statement on obtaining consent of a non-English speaking person to assist in the eyewitness identification process. Law enforcement personnel should consider arranging for an interpreter if a person interviewed:

- i. Is unable to communicate in English
- ii. Has a limited understanding of English

- iii. Is deaf, hearing impaired or speaking impaired
- iv. Is otherwise physically challenged to communicate in English

c. Review and Explain Forms

If the person is unable to read or write, the administrator, in the presence of the witness, will give the explanation, read any forms, and obtain consent and acknowledge the consent on the Witness Certification Statement, stating why the person was unable to sign the form.

4. Documentation

To strengthen the evidentiary value of the administration, it should be documented in full. Video documentation (with audio) is the preferred method. Audio recording is the preferred alternative. If neither method is employed, then the reason for not video or audio recording should be documented. A still photograph of everyone in the live lineup should be taken and details of all persons present during the live lineup should be documented.

E. Standard Operating Procedures for Show-ups

Show-ups should be avoided whenever possible because of their suggestiveness. Photo arrays and live lineups are preferred. However, where circumstances require the prompt display of a suspect to a witness, the following procedures should be followed to minimize potential suggestiveness.

1. Preparation

a. Contact Among Witnesses

Separate witnesses and do not allow communication between them before or after conducting a show-up.

b. Document Witness's Description of Perpetrator

Document the witness's description of the perpetrator prior to conducting the show-up.

c. Temporal and Spatial Proximity to the Offense

Use show-ups only where the suspect is detained within a reasonably short time frame following the offense and is found in relatively close to the scene. Although this is dependent on the individual circumstances of each case, courts have generally held that a two-hour time lapse is acceptable.

d. Transport Witness to Suspect

Transport the witness to the location of the suspect whenever practical, rather than bringing the suspect to the witness. The suspect may be taken to a location where the witness can view the suspect for possible identification.

e. Do not Return Suspect to Crime Scene

Suspects should not be taken to the scene of the crime.

f. Disclosure of Location of Witness's Home

Consider carefully whether to take the suspect to the witness's or victim's home.

g. Avoid Appearance of Guilt

Do not conduct show-ups when the suspect is in a patrol car, handcuffed, or physically restrained by police officers unless such protective measures are necessary to ensure safety.

h. Minimize Reliance on Show-ups

If one witness identifies the suspect, you are strongly urged to use a photo array or a live lineup with any remaining witnesses.

2. Administration

a. Instruct Witness

Each witness should be instructed outside the presence of the other witnesses. The show-up administrator should give the witness a written copy of the following Witness Certification Statement and should read the instruction statement aloud at the beginning of the show-up identification procedure:

**In a moment, I am going to show you a person who may or may not be the person who committed the crime.  
You should not feel you have to make an identification. It is as important to exclude innocent persons as it is to identify the perpetrator. The investigation will continue whether or not you make an identification.  
Because you are involved in an ongoing investigation, in order to prevent damaging the investigation, you should avoid discussing this identification procedure or its results.  
Do you understand the procedure and the instructions I have given you?**

b. Presentation of Suspect and Questioning of Witness

Present the suspect to the witness and ask the witness whether the person they are looking at is the person they saw commit the crime.


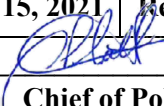
If the witness answers "Yes," ask the witness to describe, in their own words, how certain they are.

- c. Document Witness's Response  
Document the witness's response using the witness's own words.
  - d. Multiple Identification Procedures with Same Witness  
Avoid multiple identification procedures in which the same witness views the same suspect more than once.
  - e. Avoid Requirement of Performance by the Suspect  
Do not require show-up suspects to put on clothing worn by, speak words uttered by, or perform other actions of the perpetrator.
  - f. Avoid Conduct Suggestive of the Suspect's Guilt  
Officers should avoid words or conduct that may suggest to the witness that the individual is or may be the perpetrator.
  - g. Contact Among Witnesses  
Remind the witness not to talk about the show-up to other witnesses until police or prosecutors deem it permissible.
3. Special Procedures are Required for Illiterate Persons or Persons Who Possess Limited English Proficiency
- a. Be Alert to People Who do not Speak English or Possess Limited English Proficiency  
Given the diversity of communities, police officers may encounter persons who do not speak English or who possess limited English proficiency during a criminal investigation. Where presented with this situation, officers should carefully consider the ethical and legal ramifications of how to handle the case when there is a language barrier.
  - b. Using an Interpreter  
Unless the show-up administrator speaks the victim's or witness's language fluently, an interpreter should be used for persons who do not speak English. Law enforcement personnel should consider arranging for an interpreter if a person interviewed:
    - i. Is unable to communicate in English
    - ii. Has a limited understanding of English
    - iii. Is deaf, hearing impaired, or speaking impaired
    - iv. Is otherwise physically challenged to communicate in English



#### 4. Documentation

To strengthen the evidentiary value of the administration it should be documented in full including the time, date, and location of the procedure, identities of persons present, and the outcome of the procedure. Video documentation (with audio) is the preferred method. Audio recording is the preferred alternative. If neither method is employed, then the reason for not video or audio recording should be documented.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.43 Informants</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 7.11 and 7.12	

## I. POLICY

In many instances, a successful investigation cannot be conducted without the use of confidential informants or CIs. While the use of CIs is an effective tool in investigations, it can be undermined by the misconduct of the CI or the officer utilizing the informant. Therefore, it shall be the policy of this law enforcement agency to take necessary precautions by developing sound informant-control procedures.

## II. PURPOSE

The purpose of this policy is to provide regulations for the control and use of confidential informants (CIs).

## III. DEFINITIONS

- A. Confidential Informant: An individual who provides services or information to the police, with or without being paid, but who wishes to remain anonymous.
- B. Confidential Informant File: File maintained to document all information that pertains to confidential informants.

## IV. PROCEDURES

- A. Establishment of an Informant File System
  - 1. Sergeants shall be responsible for developing and maintaining confidential informant files.
  - 2. A file shall be maintained on each confidential informant (CI) used by officers. Each file shall be coded with an assigned informant control number and shall contain the following information:
    - a. Informant's name
    - b. Informant payment record, which provides a summary of informant payments and which is kept on top of the file

- c. Receipts for purchase of information.
  - d. Copy of each statement made by informant.
  - e. Name of officer initiating use of the informant.
  - f. Informant's photograph, fingerprints, and criminal history record.
  - g. Briefs of information provided by the CI and its subsequent reliability.
  - h. Signed informant agreement.
  - i. Update on active or inactive status of informant.
3. If it is determined that an informant is unreliable, the informant's file shall be placed in the "Unreliable Informant File."
  4. All persons determined to be unsuitable for use as a CI shall be referenced as "unreliable" in the Informant File.
  5. Confidential informants who at any time provide officers with false or erroneous information or statements shall have the notation "Unreliable" and the details of the erroneous information placed in the CI file. Officers shall not use any information provided by an individual who has previously been designated an unreliable informant.
  6. Informant files shall be maintained in a secured area within the Sergeants Office.
  7. Access to the informant files shall be restricted to the Chief of Police and the Sergeants, or their designees.
  8. Sworn personnel may review an individual's informant file only with the approval of the Chief of Police or Sergeant overseeing the Confidential Informant File.

#### B. Recruitment and Use of Informants

It is critical that officers exercise good judgment in their use of informants, and that they understand the motivation that prompts an individual to serve as an informant. The most common motives include providing information to eliminate or reduce a criminal case against themselves, for money, and a sense of civic responsibility. But there might be other reasons, making it important that officers ascertain the true motive.

1. Officers may recruit informants in the following manner:
  - a. From the members of the public who may have information about specific criminal activities occurring in the city.

- b. From individuals arrested for non-violent crimes, such as possession of controlled substances. No CIs will be recruited for purposes of reducing or eliminating any charges where there is a victim of a crime or charges involving family violence.
  - c. From individuals who volunteer to be a CI, with or without payment.
  - d. Juveniles (under the age of 21) shall not be used. While officers may receive information and act on confidential information given by a juvenile, the juvenile shall not be considered a CI nor encouraged nor paid any monies (other than through the Crime Stopper program) for any work done. The use of juveniles for tobacco or alcohol sting operations is permitted if approved by the Chief of Police and with the approval signature of custodial parents.
2. Before using an individual as a CI, an officer must receive initial approval from the Sergeant.
  3. Before using any individual, who is currently on probation or parole, the officer must obtain written permission from the controlling probation or parole officer.
  4. The officer shall compile information through a background investigation that is sufficient to determine the reliability and credibility of the individual. Any person convicted of moral turpitude crimes will be deemed “unreliable” and, therefore, not be utilized as a CI.
  5. After the officer receives initial approval to use an individual as a CI, an informant file shall be opened.

#### C. General Guidelines for Handling CIs


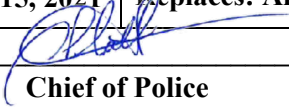
1. All CIs are required to sign and abide by the provisions of the departmental informant agreement. The officer utilizing the CI shall discuss each of the provisions of the agreement with the CI, with emphasis on the following:
  - a. Informants are not law enforcement officers. They have no arrest powers, are not permitted to conduct searches and seizures, and may not carry a weapon.
  - b. Informants will be arrested if found engaging in any illegal activity, and they will receive no special legal considerations.
  - c. Informants are not to take, and the department will not condone, any actions that may be considered entrapment. Entrapment occurs when the informant encourages, persuades, or otherwise motivates a person to engage in criminal activity.
2. No member of this agency shall knowingly maintain a social relationship with CIs while off duty, or otherwise become personally involved with any CIs. Members of this agency shall not solicit any favors, accept gratuities from, or engage in any private business transaction with any CI. Any violations of this provision will subject the officer to disciplinary action, up to and including termination.

3. Whenever possible, an officer shall be accompanied by another officer when meeting with a CI.

#### D. Payments to Informants

1. The department maintains a confidential fund for payment to informants. Payments to informants (CIs) will be approved by the Chief of Police in advance of any payment.
2. Officers wishing to secure the services of a paid informant shall do the following: prepare and present to his or her supervisor a Request-for-Funds form with the CI's number, a short explanation of what information is being purchased, and what case or incident the information pertains to. The supervisor will determine if the payment is appropriate and forward the request to the Chief of Police.
3. Payment can be requested the following purposes: information alone; investigative funds for the purchase of illegal drugs, contraband and other criminal evidence; purchases of food and beverages for a confidential informant; expenditures for authorized undercover operations; and flash and front money.
  - a. If the expenditure is approved by the Chief of Police, the Sergeant will log out the money to the officer and have the officer sign a receipt for the money on the Request Form. The Sergeant shall also note the disbursement in the confidential funds log.
  - b. The officer will meet with the informant with at least one other officer or supervisor present and obtain the information and make payment to the CI. The CI will sign a receipt for the funds.
  - c. If no payment is made, the funds will be returned to the Sergeant before the end of shift.
  - d. The receipt will be returned to the Sergeant along with a summary of the information provided and will place the original of the receipt in the confidential fund log.
  - e. A copy of the receipt and the summary of information given will be placed in the CI's file.
4. Narcotics Informants
  - a. Payment for any covert drug purchase should follow all standard protocols for proving reliance, including searching the informant prior to the purchase, providing only purchase cash, surveillance to and from the purchase, and a complete search following the purchase, witnessed by at least two officers.
  - b. If possible, a single CI should not be allowed to identify a narcotics target and make a purchase for the prosecution of that target. A separate CI should be used if possible, to prevent a CI from using the law-enforcement system to his/her advantage.

5. Maintenance of the confidential fund. (TEXAS BEST PRACTICES: 7.12)
  - a. The Sergeant is assigned the responsibility for maintaining the informant fund. The fund will be maintained in a locking cash box that is kept locked in the safe in the Chief's office.
  - b. At no time will there be more than \$500 in the informant fund.
  - c. The confidential fund custodian shall make payments only to those who have approval from the Chief of Police or a designee.
  - d. The custodian is not permitted to make disbursements from the confidential fund to himself/herself.
  - e. A disbursement log and receipt book will be maintained inside the cash box with the funds. Entries in the log will be made for every disbursement or return as well as replenishment of the fund.
  - f. The disbursement log shall record the beginning balance, date of withdrawal, amount, name of receiving officer, CI number, case number if any, and ending balance.
  - g. After an officer returns with a receipt signed by the informant, the CID supervisor will check the signature to ensure a match with the signature on file and place a copy of the receipt in the informant file along with a statement of the information or service received. The original of the receipt will be kept in a file in the safe with the cash box.
  - h. When the amount in the informant fund drops below \$100, the Sergeant will request replenishment from the Chief of Police, who will request replenishment from the City Bookkeeper or City Administrator.
  - i. At least every six months, the Chief of Police or a designee not connected with the management of the fund will conduct an audit of the fund and operational procedures. The audit will be documented and forwarded to the Chief of Police and the City Bookkeeper or City Administrator. A notation of the audit will also be made in the disbursement log.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 7.44 Sex Offender Registration</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 7.31</b>	

## I. POLICY

Police departments are required by law to register sex offenders who intend to reside within their jurisdiction. Citizens of our city expect the department to be protective of their children by registering sex offenders and ensuring they comply with the terms of their court-imposed requirements. The Teague Police Department will meet those expectations by accurately registering sex offenders, conducting periodic checks to ensure offenders are complying with the court's requirements, and prosecuting those who fail to do so.

## II. PURPOSE

The purpose of this policy is to define procedures for sex-offender registrations and compliance checks.

## III. PROCEDURES

### A. Sex-Offender Registration


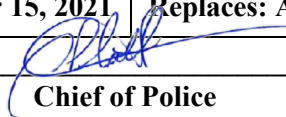
1. The Chief of Police, or his designee, conducts all sex-offender registrations.
2. Sex-offender registrations require the following steps:
  - a. The Texas Department of Public Safety Sex Offender registration form INT-10 is completed.
  - b. Two DPS fingerprint cards are completed.
  - c. Two photographs are taken of the offender.
  - d. Two photographs are taken of the offender's vehicle.
  - e. The white copy of the INT-10, one photograph, and one fingerprint card are sent to the Texas DPS Criminal Intelligence Service.

- f. The canary copy and the pink copy of the INT-10 form, one photograph, and one fingerprint card are placed in the offender's folder, which is maintained in the Sexual Offender File.
3. The registration and notification from the Department of Criminal Justice, as well as the original offense information if necessary, are reviewed for the notifications to educational institutions and the public as currently required under the Code of Criminal Procedure.
4. Texas CCP 62.054 Circumstances Requiring Notice to Superintendent or School Administrator governs when such notice is given. When required, the notice shall be completed on the form prescribed by the Chief of Police and mailed to each public or Private Primary or Secondary School within our jurisdiction.

#### B. Sex-Offender Compliance Checks

1. Under CCP 62.06, sex offenders subject to registration are also required to report periodically and at a frequency dependent upon the number of convictions. The department shall maintain a schedule to ensure these offenders report as required. If an offender fails to report properly, the department shall investigate to determine if a violation has occurred.
2. At least annually, department personnel will contact registered sex offenders and update the offender's file with the following:
  - a. A new photograph.
  - b. A new photograph and the license number of any vehicles the offender owns or has access to.
  - c. New employment information.
  - d. Any new descriptive information (weight, scars, tattoos, etc.).
3. If the offender cannot be located, an investigation will be conducted to determine if terms of registration have been violated. If so, a criminal case will be filed, and a warrant issued.



	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 8.0 Unusual Occurrences and Special Events</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 2.22, 8.07, 8.08, 8.09, and 8.11	

## I. POLICY

Unusual occurrences include emergencies resulting from natural or man-made disasters or civil disturbances, such as riots, disorders, spontaneous violence, or labor disputes. While these occurrences are uncommon, the department must always be prepared to deploy personnel in the field and to coordinate with the responses of other law-enforcement agencies and other public service agencies that might become involved. Department personnel must act quickly, decisively, and knowledgeably to mitigate disorder or disaster by restoring order and control, and by protecting lives and property.

## II. PURPOSE

The purpose of this policy is to establish general guidelines for planning and deploying personnel for unusual occurrences.

## III. DEFINITIONS

- A. Unusual Occurrences: Natural or man-made disasters, civil disturbances, unusual police situations, such as hostage taking or barricaded persons, and even planned or unplanned major incidents. (TEXAS BEST PRACTICES 8.08)
- B. After-Action Reports: A report outlining the department’s planning and response to an unusual occurrence, providing a critical look at operations, and developing suggestions for future planning and policy issues.
- C. Emergency Response Plan: A county or regional emergency response plan that outlines the responsibilities of all public agencies in time of natural or man-made disasters or any other unusual occurrence that requires special action by this agency.
- D. Major Incident: In this context – An unplanned major event of significant public or community interest that requires an extraordinary response by the police. Typically, these are unexpected mass gathering fueled by a common concern or theme that result in multiple arrests and/or property damage. Examples include, but are not limited to: unplanned or unpermitted gatherings that lead to civil disobedience and are focused on the action(s) of police personnel (e.g.: a controversial officer-involved incident), or an

unexpected celebratory crowd that turns riotous or destructive (e.g.: a crowd celebrating a sports event that degrades to property damage and mass arrest).

#### **IV. PROCEDURES**

##### **A. Administration**

1. The Chief of Police is responsible for the overall planning of the law-enforcement response to unusual occurrences and for department participation in the regional emergency operation plan.
2. The Chief of Police is responsible for coordinating all law-enforcement plans with the municipal, county, or state officials charged with emergency activities.
3. A copy of the emergency operations plan will be maintained in the office of the Chief, the supervisor's office, and in the patrol briefing room. (TEXAS BEST PRACTICES: 8.07)
4. At least once annually, the department shall conduct training for all personnel on their roles and responsibilities under the county emergency response plan.
5. At least annually, the Chief of Police will require an internal review of the law-enforcement appendix to the emergency response plan and other departmental procedures for unusual occurrences. (TEXAS BEST PRACTICES: 8.09)

##### **B. Special events**

1. The Chief of Police is responsible for the proper planning of the law-enforcement operations for any special event held within the city.
2. At a minimum, special event plans shall include the following:
  - a. Anticipated personnel needs and assignments.
  - b. Special qualification requirements, if any.
  - c. Command structure.
  - d. Written estimates of traffic, crowd, or crime problems anticipated.
  - e. Clearly written traffic flow plans.
  - f. Logistics requirements.
  - g. Coordination with outside agencies.
3. Handling of Civil Disturbances is covered in Policy 8.2.

### C. Unusual Police Incidents

1. Unusual police incidents include the following:
  - a. Bomb threats or incidents where an evacuation is performed, or a device is located.
  - b. Hostage taking where the victim is held after police arrival.
  - c. Barricaded persons with Emergency Response Teams callout.
  - d. Hazardous warrant service.
  - e. Other major incidents where more than three units and a supervisor are utilized.
2. The Chief of Police is notified immediately if any unusual police event occurs.
3. Patrol standard operating procedures provide officers direction in handling many unusual police incidents.
4. The management and use of the ERT is provided in Policy 8.3.

### D. Use of National Incident Management System (NIMS)

1. The department trains all personnel in their appropriate level of NIMS courses for understanding of their role in the management of an incident. (TEXAS BEST PRACTICES: 8.11)
2. The NIMS process of incident command will be utilized in handling all unusual occurrences where more than three units are utilized.


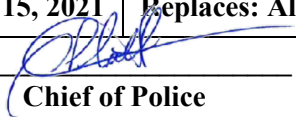
### E. Mobilization of Additional Resources

1. In any emergency or special operation where law-enforcement resources in addition to regular duty personnel are required, the Chief of Police may take one or more of the following actions:
  - a. Hold over the shift due to go off so that personnel from two shifts are available.
  - b. Call back additional personnel.
  - c. Request assistance through mutual aid.
  - d. Request that the mayor ask for state assistance through the governor's office.
2. Some special operations are planned weeks in advance and, where possible, additional personnel required will be given advance notification of time, place, uniform, duties, etc. For other operations, such as raids, security considerations may limit advanced notification to minutes.

3. All members of the department are subject to immediate recall in the event of an emergency.
4. Failure to respond to an order to report to work shall be grounds for termination. (TEXAS BEST PRACTICES: 2.22)
5. The Chief of Police shall assign personnel called back as required, using the skills, knowledge, and abilities of individual recalled officers as needed.
6. Call-back time is paid time and will be strictly controlled and accounted for, minimizing expenditure where feasible.

F. After Action Reports (TEXAS BEST PRACTICES: 8.08)

1. After-action reports are required at the conclusion of any unusual occurrence within 10 days of end of the event.
2. Unless otherwise assigned, the supervisor in charge of the event is responsible for the preparation of the report.
3. The after -action report should include the following:
  - a. A detailed, chronological description of the event.
  - b. A description of the prior planning for the event, if any.
  - c. The number and identity of personnel assigned.
  - d. A discussion of the event with focus on the problems encountered or successes accomplished.
  - e. A critical review of operations and what policy, equipment, or procedures need to be changed so that the department can improve its response to a similar problem or event in the future.
4. The after-action report should be prepared in memorandum format and forwarded to the Chief of Police for review.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 8.1 Civil Disturbances and Mass Arrests</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: Texas Best Practices 8.07</b>	

## I. POLICY

How law-enforcement officers interact with crowds in civil actions, whether in demonstrations or civil disturbances, has direct bearing on their ability to prevent property damage, injury, or loss of life, and to minimize disruption to persons who are uninvolved. Officers confronting civil disturbances and those called upon to assist in these incidents shall follow the procedures as enumerated in this policy to protect life, property, and first amendment rights.

In rare circumstances resulting from man-made or natural emergencies, and in widespread, highly volatile civil unrest with the potential for widespread violence, the incident commander may temporarily deviate from any policy, provision, or guideline contained herein when such action is determined to be the only reasonable alternative for the prevention of loss of life or major property damage.

It is critical to remember that the Constitution of the United States (and other important, binding documents and court decisions) afford the right of the people to express themselves in a variety of ways and for an almost infinite number of reasons. It is the policy of this police department that all human rights are respected and supported.

Further, this department will not provoke or incite demonstrators through any unnecessary show of force. Incident commanders will rely on their training and experience when faced with hostile crowds and will consult (when they are able) with the Chief of Police or appropriate on scene commanders.

It is the policy of this department to avoid making mass arrests of persons when arrest avoidance is reasonable in the interests of safety and security. In addition, this department is committed to working with demonstrators to explore a peaceful and reasonable solution to prevailing concerns.

## II. PURPOSE

The purpose of this policy is to establish guidelines for managing crowds and preserving the peace during demonstrations and civil disturbances.

### **III. DEFINITIONS**

- A. **Civil Disturbance:** An unlawful assembly, as defined by state statutes and local ordinances. Normally, a gathering that constitutes a breach of the peace or any assembly of persons where there is a threat of collective violence, destruction of property, or other unlawful acts. These are typically, but not always, spontaneous occurrences requiring the emergency mobilization of police forces and related emergency services.
- B. **Demonstration:** A legal assembly of persons organized primarily to express a political position or other doctrinal view. These are typically scheduled events that allow for police planning. They include but are not limited to marches, protests, and other assemblies that are largely designed to attract the attention of onlookers, media, and others. Demonstrations can evolve into civil disturbances that necessitate enforcement actions. Although crowd control may be necessary at sporting events, festivals, concerts, celebratory gatherings, and related events, these are not defined as demonstrations.
- C. **Crowd Control:** Techniques used to address unlawful public assemblies, to include a show of force, crowd containment, dispersal equipment, and strategies, and preparations for multiple arrests.
- D. **Crowd Management:** Techniques used to manage lawful assemblies before, during, and after the event for the purpose of maintaining their lawful status as accomplished through event planning, pre-event contact with group leaders, issuance of permits, intelligence gathering, personnel training, and other means.
- E. **Skip-Fired Projectiles:** Weapons that are discharged toward the ground in front of a target to bounce to the target.

### **IV. PROCEDURES: General Management and Organization Principles**

- A. By law, this municipality may impose reasonable restrictions on the time, place, and manner of expressing first amendment rights. This department shall place only those limitations and restrictions on demonstrations necessary to maintain public safety and order and, to the degree possible, allow uninhibited commerce and freedom of movement for uninvolved persons. If possible, any planned constraints of first amendment rights will be reviewed by city legal prior to implementation.
- B. The on-duty supervisor will assume the role of incident commander (IC) at the scene of mass demonstrations and civil disturbances until relieved by a higher-ranking supervisor or the Chief of Police.
- C. Emergency Operations Plan (TEXAS BEST PRACTICES 8.07) – will be made available to all command staff and communications staff, and will at a minimum include provisions for the following:
  - 1. Civil disturbance

2. Mass arrest
  3. Response to natural and manmade disasters
  4. Uniform and equipment usage
  5. Use of less-lethal weapons
  6. Use of canine and horses
  7. Overall goal of incident management
- D. The commander of the emergency response team shall be responsible for preparing any tactical plans and management details associated with planned demonstrations.
- E. If possible, a member of the department should be detailed to conduct a video recording of the incident and the department's response to it, including any interactions involving use of force.
- F. The incident-command system shall be used in crowd management and civil disturbances to ensure control and unified command. The incident commander shall do the following:
1. Assume responsibility for issuing and disseminating all orders to members of his or her command and for determining the resources that are necessary and the extent to which they will be used.
  2. Direct the establishment and organization of an incident command post.
  3. Call for any necessary assistance.
  4. Authorize such use of force and engagement with the crowd as deemed necessary to resolve unlawful actions.
  5. Authorize the use of arrest as a means of curtailing unlawful behavior.
  6. Designate a liaison officer to coordinate with other city or county emergency service providers as well as government offices, agencies, and departments.
  7. Ensure that officers at the staging area are briefed on the type of crowd being monitored. They will be told what to expect from participants and what types of responses and force can be employed. They shall also be informed that the incident commander will order the response deemed appropriate and that the unit will act in concert with and follow the direction of the incident commander.

## V. USE OF FORCE

- A. The department's use-of-force policy is equally applicable to enforcement actions in the context of both mass demonstrations and civil disturbances. That is, officers may use only such force as reasonably appears necessary to protect themselves or others from physical harm, to restrain or subdue a resistant individual, or to bring an unlawful situation safely and effectively under control.
- B. Unity of action, command, and control are key to effective handling of demonstrations and civil disturbances. Thus, unless exigent circumstances require immediate action, officers shall not independently make arrests or employ force without command authorization. In exigent circumstances, supervisors shall independently authorize the use of force or such other tactics in accordance with the agency's use-of-force policy and this policy.
- C. All officers helping this agency through mutual aid agreements, contracts, or other means shall be briefed on the mutually agreed upon provisions of those agreements relating to the use of force and protocols for crowd control prior to deployment.
- D. The following restrictions and limitations on the use of force shall be observed during mass demonstrations and civil disturbances:
  - 1. Canine teams may respond as backup as appropriate, but officers shall not deploy dogs for crowd control. Canines shall remain in patrol vehicles or other secure locations and, whenever reasonably possible, out of the view of demonstrators. Canines may be deployed in isolated circumstances related to pursuit of suspects in buildings and related environments.
  - 2. Horses may be used to surround and control groups in nonviolent demonstrations as appropriate. They shall not be used against passively resistant demonstrators who are sitting or lying down. Horses shall not be deployed when the use of chemical agents is anticipated or deployed, nor shall they be used in icy or snow conditions.
  - 3. Fire hoses shall not be used for crowd containment or dispersal.
  - 4. Motor vehicles may be used to surround and move persons as appropriate but shall not be brought into contact with them for purposes of containment or dispersion.
  - 5. Less lethal projectiles shall not be fired indiscriminately into crowds. Skip-fired projectiles and munitions or similar devices designed for non-directional, non-target-specific use may be used in civil disturbances where life is in jeopardy.
  - 6. Direct-fired impact munitions, to include beanbag and related projectiles, shall not be used for crowd control or management during demonstrations.
  - 7. Direct-fire munitions may be used where reasonable during civil disorders against specific individuals who are engaged in conduct that poses a threat of death, great



bodily harm, or serious property damage, when the individual can be properly targeted.

8. When reasonably possible, a verbal warning shall be issued prior to the use of impact munitions.
9. Electronic control weapons (ECW) shall be used during civil disturbances only for purposes of restraint or arrest of individuals who are actively resisting and when alternative, lesser means of control are not available or are unsuitable and only when an individual can be accurately targeted. ECWs may not be fired indiscriminately into crowds.
10. Officer-issued aerosol restraint spray (OC) may be used against specific individuals who are engaged in unlawful acts or conduct or are actively resisting arrest, or as necessary in a defensive capacity when other alternatives would likely be inadequate or are unavailable. It shall not be used indiscriminately against groups of people, in demonstrations or crowds where bystanders would be unreasonably affected, or against passively resistant individuals.
11. High-volume OC delivery systems, such as MK-9 and MK-46, are designed for use against groups of people engaged in unlawful acts or ones who are endangering public safety and security. These may be used only with the approval of the incident commander. Whenever reasonably possible, a warning shall be issued prior to the use of these systems.
12. CS chemical agents are primarily offensive weapons that shall be used with the utmost caution. CS may be deployed defensively to prevent injury when lesser force options are either not available or would likely be ineffective. Such munitions shall be carried and deployed only by trained and authorized officers at the direction of the incident commander or field commander and only when avenues of escape are available to the crowd and, where possible, announced to the crowd in advance. Whenever reasonably possible, a warning shall be issued prior to the dispersal of chemical munitions. Chloroacetophenone (CN or "Tear gas") may not be used in any instance.
13. The riot baton shall be used primarily as a defensive weapon or as a means of overcoming active resistance. It is used in the two-hand horizontal thrust on a police line, as a show of force, or to contain or disperse a crowd.

#### E. Use-of-Force Reporting and Investigation

Established use-of-force reporting requirements of this department are equally applicable to policing mass demonstrations and civil disturbances. However, reporting, documenting, and recording uses of force in the context of civil disturbances and mass demonstrations can be hampered by logistical and safety concerns. Officers will complete use-of-force forms as soon as practical after the event.

## VI. DEMONSTRATIONS

- A. Preparation for responding to a demonstration is the responsibility of the Chief of Police. The incident commander shall ensure that a written, incident-action plan is developed for approval by the Chief or his or her designee.
  
- B. Every effort shall be made to identify the leaders of the demonstration and to contact these leaders in advance of the demonstration. A decision on personnel, resources, and related needs shall be based in part on information obtained from leaders, department intelligence, and other sources. In addition, answers to the following questions, and other related questions, shall be collected:
  - 1. What type of event is involved?
  - 2. When is it planned?
  - 3. Is outside opposition to the event expected?
  - 4. How many participants are expected?
  - 5. What are the assembly areas and movement routes?
  - 6. What actions, activities, or tactics does the department anticipate the demonstrators will use, including devices designed to thwart arrest?
  - 7. Have permits been issued?
  - 8. Have other agencies, such as fire and EMS, been notified?
  - 9. Is there a need to request mutual aid?
  - 10. Will off-duty personnel be required?
  - 11. Have demonstration leaders been identified, and, if so, what is their history of conduct at such events?
  - 12. Is it possible to meet with group leaders?
  
- C. Based on this and related information, the department will develop an action plan together with outside agencies where necessary. The plan shall address provisions for the following and be distributed to all affected command and supervisory officers.
  - 1. Command assignments and responsibilities
  - 2. Manpower, unit structure, and deployment
  - 3. Liaison with demonstration leaders

4. Liaison with outside agencies
  5. Release of information to the news media
  6. Transportation, feeding, and relief of personnel
  7. Traffic management
  8. Demonstrator devices, extrication teams, and equipment
  9. First aid stations
  10. Transportation of prisoners
  11. Prisoner detention areas
  12. Any intelligence information
- D. Officers shall monitor crowd activity. Sufficient resources to make multiple simultaneous arrests should be available, depending on the fluidity of the situation and degree of actual or likely disruption.
- E. Assigned officers shall always wear their badges and nameplates or other identification on the outside of their uniforms or on their helmets.
- F. Officers shall be positioned in such a manner as to minimize contact with the assembly.
- G. Officers shall not engage in conversations related to the demonstration or react to comments from demonstrators.
- H. Officers shall maintain a courteous and neutral demeanor.
- I. Persons who reside, are employed, or have business of an emergency nature in the area marked off by a police line shall not normally be barred from entering the demonstration area unless circumstances suggest that their safety would be jeopardized or their entry would interfere with police operations.
- J. Unit commanders shall establish and maintain communication with demonstration leaders and relay information on crowd mood and intent to the incident commander. Supervisors shall maintain close contact with officers under their charge to ensure their compliance with orders, to monitor their behavior and disposition, and to ensure that they are aware of any changes in crowd attitude or intent.
- K. Before ordering forced dispersal of demonstrators, the incident commander shall determine whether lesser alternatives may be effective. These alternatives include the use of containment and dialogue, as follows:

1. Establish contact with crowd leaders to assess their intentions and motivations and develop a mutually acceptable plan for de-escalation and dispersal
2. Communicate to the participants that their assembly is in violation of the law, that the department wishes to resolve the incident peacefully, but that acts of violence will be dealt with swiftly and decisively
3. Negotiate with crowd leaders for voluntary dispersal or target specific violent or disruptive individuals for arrest. Prior to issuing dispersal orders, the incident commander shall ensure that all potentially necessary law enforcement, fire, and EMS equipment and personnel are on hand to successfully carry out tactical requirements for all contingencies, and that logistical requirements related to the potential for making mass arrests are in place.
4. When the incident commander has determined that crowd dispersal is required, he or she shall direct unit commanders to issue warnings prior to taking physical actions to disperse the crowd if time and circumstances permit,
5. The warnings shall be issued loudly enough and often enough to be heard by the crowd from stationary vantage points or with the use of public address devices in moving patrol vehicles.
6. The warning shall consist of an announcement citing the offenses or violations being committed, an order to disperse, and designated dispersal routes. A second and a third warning shall be issued at reasonable time intervals before designated actions are taken to disperse the crowd. Where possible, the warnings shall be audio- or video-recorded at a point to the rear of the crowd, and the time and the names of the issuing officers recorded in the Incident Commander's event log.
7. Specific crowd-dispersal tactics shall be ordered as necessary where the crowd does not heed warnings. These include any one or any combination of the following:
  - a. Display of forceful presence to include police lines, combined with police vehicles and mobile field forces.
  - b. Crowd encirclement
  - c. Multiple simultaneous arrests
  - d. Use of aerosol crowd-control chemical agents
  - e. Police formations and use of batons for forcing crowd movement

## **VII. SPONTANEOUS DEMONSTRATIONS AND CIVIL DISTURBANCES**

- A. Demonstrations or large gatherings of any kind that escalate into disturbances are governed by the policies and regulations concerning crowd management, control, and dispersal as identified here with respect to civil disturbances. The first officer to arrive on the scene of a spontaneous demonstration or civil disturbance shall do the following:
1. Observe the situation from a safe distance to determine if the gathering is currently or potentially violent.
  2. Notify the communications center of the nature and seriousness of the disturbance, particularly the availability of improvised or deadly weapons, its location and estimated number of participants, current activities (such as blocking traffic), direction of movement, and ingress and egress routes for emergency vehicles.
  3. Request the assistance of a supervisor and any necessary backup and advise as to the present course of action.
  4. If approaching the crowd would not present unnecessary risk, instruct the gathering to disperse.
  5. Attempt to identify crowd leaders and agitators and anyone engaged in criminal acts
- B. The first field supervisor in charge at the scene shall assess the situation and request sufficient personnel and related resources to perform the following tasks:
1. Deploy officers to the best vantage points to observe and report on crowd actions.
  2. Establish an outer perimeter sufficient to contain the disturbance and prohibit entrance into the affected area.
  3. Ensure that, to the degree possible, uninvolved civilians are evacuated from the immediate area of the disturbance.
  4. Establish a temporary command post based on proximity to the scene, availability of communications, space, and security from crowd participants.
  5. Continually assess the situation and advise communications of any change in status and any additional needs.
  6. Ensure that surveillance points are established to identify agitators, leaders, and individuals committing crimes, and to document and report on events as they happen.
  7. Where illegal gatherings engaged in civil disturbances cannot be controlled with available field personnel within a reasonable time frame, the Chief of Police or his or her designee shall serve as or appoint an IC to direct operations.

8. The primary objectives of the IC will be as follows:
  - a. Protect persons, including nonparticipants and participants alike, and property at risk.
  - b. Disperse disorderly or threatening crowds to eliminate the immediate risks of continued escalation and further violence.
  - c. Effect the arrest of those individual law violators and the removal or isolation of those persons inciting violent behavior.
  - d. To achieve the foregoing objectives, the IC shall employ tactical operations that include but are not necessarily limited to approaches previously identified in this policy.
  - e. In the area outside the perimeter surrounding the disorder site, the IC shall ensure that the following actions are taken.
  - f. Move and reroute pedestrian and vehicular traffic around the disorder.
  - g. Limit access to the disorder to those persons approved by the IC or other commander.
  - h. Control unauthorized egress from the disorder by participants.
  - i. Repulse attempts to assist or reinforce the incident participants from outside the area.
  
9. The IC shall also ensure the following matters are addressed where indicated:
  - a. Ensure that adequate security is provided to fire and EMS personnel in the performance of emergency tasks.
  - b. Ensure that feeding and relief requirements of personnel have been addressed.
  - c. Ensure the adequacy and security of the incident command post and designate a staging area for emergency responders and equipment.
  - d. Establish liaison and staging point for media representatives and, to the degree possible, provide them with available information.
  - e. Ensure that the IC's event log is staffed for documenting activities and actions taken during the incident.
  - f. Take photographs and make video-recordings of event proceedings.
  - g. Take photographs of any injuries sustained by police officers or the public.

- h. Determine the need for full mobilization of sworn officers and the recall of off-duty officers.


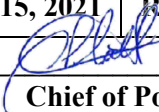
## **VIII. MASS ARRESTS**

- A. During civil disturbances, it may be necessary to make arrests of numerous individuals over a relatively short period of time. For this process to be handled efficiently, safely, and legally, the following shall be observed:
  1. Except for felony offenses, officers shall not pursue demonstrators into buildings for the purpose of making arrests unless specifically instructed to do so by a supervisor. Supervisors shall accompany and exercise control over members under their command who go on private property or enter buildings to make arrests.
  2. Designated, supervised squads of officers shall perform mass arrests.
  3. If required, an adequate secure area shall be designated for holding prisoners after arrest and while awaiting transportation.
  4. Arrest teams shall be advised of the basic charges to be recorded in all arrests.
  5. Arrestees who are sitting or lying down but agree to walk shall be escorted to the transportation vehicle for processing. Two or more officers shall carry those who refuse to walk.
  6. At the transport vehicle, the arrestee shall be advised of the charges. The prisoner shall be searched for weapons, evidence, and contraband, and where possible, by an officer of the same sex. Such items shall be secured and identified prior to transportation.
  7. Photographs shall be taken of the arrestee with the arresting officer, and of the prisoner and any property that is turned over to the transporting officer. Transporting officers shall not accept prisoners without a properly prepared field arrest form and photographs and shall ensure that all property is placed in a container that is legibly marked with the arrested person's information.
  8. Upon arrival at the detention facility, the transporting officer shall deliver the prisoner together with the arrest form and personal property.
  9. All injured prisoners and those who request medical attention shall be provided medical attention prior to transportation to the detention facility.
  10. Photographs shall be taken of all injuries.
- B. All arrested juveniles shall be handled in accordance with this department's procedures for the arrest, transportation, and detention of juveniles.

## **IX. DEACTIVATION**

- A. When the disturbance has been brought under control, the IC shall ensure that the following measures are taken:
  - 1. All law-enforcement officers engaged in the incident shall be accounted for, and an assessment and documentation made of personal injuries.
  - 2. Witnesses, suspects, and others shall be interviewed or interrogated.
  - 3. All necessary personnel shall be debriefed as required.
- B. All written reports shall be completed as soon as possible after the incident. They will include comprehensive documentation of the basis for the incident, the department's response to the incident, and a statement of impact that includes the cost of equipment, personnel, and other expenses related to the incident.



	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 8.2 Assisting the Mentally Ill</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b>	

## I. POLICY

It is the policy of this department to protect an emotionally or mentally unstable person from harming themselves, others, or property. Police work brings officers into contact with persons who are emotionally or mentally unstable. This instability may be due to any number of factors, including alcohol/drug dependency, emotional trauma, or some form of mental illness.

Our primary concern in these cases is the safety and welfare of that person, the community, and the officer. An officer who has probable cause to believe that an emotionally or mentally unstable person presents an immediate threat of harm to himself/herself or another person will take that person into protective custody and transport him/her to a facility where trained professionals can evaluate the emotional and mental status of that person.

## II. PURPOSE

The purpose of this policy is to provide officers with guidance on responding to calls involving the mentally ill.

## III. PROCEDURES

- A. Recognizing abnormal behavior: Mental illness is often difficult for even trained professional to define in troubled individual. Officers are not expected to make judgments of mental or emotional disturbance but rather to recognize behavior that is potentially destructive and/or dangerous either to the person or others.

The following are generalized signs and symptoms of behavior that may suggest mental illness although officers should not rule out other potential causes, such as reactions to narcotics or alcohol or temporary emotional disturbances that are situationally motivated. Officers should evaluate the following and related symptomatic behavior in the total context of the situation when making judgments about an individual's mental state and the need for intervention absent the commission of a crime.

1. Degree of Reactions. Mentally ill persons may show signs of strong and unrelenting fear of persons, places, or things. The fear of people or crowds, for example, may make the individual extremely reclusive or aggressive without apparent provocation.

2. **Appropriateness of Behavior.** An individual who demonstrates extremely inappropriate behavior for a given context may be emotionally ill. For example, a motorist who vents his frustration in a traffic jam by physically attacking another motorist may be emotionally unstable.
3. **Extreme Rigidity or Inflexibility.** Emotionally ill persons may be easily frustrated in new or unforeseen circumstances and may demonstrate inappropriate or aggressive behavior in dealing with the situation.
4. In addition to the above, a mentally ill person may exhibit one or more of the following characteristics:
  - a. Abnormal memory loss related to such common facts as name, home address, (although these may be signs of other physical ailments, such as injury or Alzheimer's disease).
  - b. Delusions, the belief in thoughts or ideas that are false, such as delusions of grandeur ("I am Christ.") or paranoid delusions ("Everyone is out to get me.").
  - c. Hallucinations of any of the five senses (e.g., hearing voices commanding the person to act, feeling one's skin crawl, smelling strange odors, etc.).
  - d. The belief that one suffers from extraordinary physical maladies that are not possible, such as persons who are convinced that their heart has stopped beating for extended periods of time.
  - e. Extreme fright or depression.
5. **Determining Danger:** Not all mentally ill persons are dangerous while some may represent danger only under certain circumstances or conditions. Officers may use several indicators to determine whether an apparently mentally ill person represents an immediate or potential danger to himself/herself, the officer, or others. These include the following:
  - a. The availability of any weapons to the suspect.
  - b. Statements by the person that suggest to the officer that the individual is prepared to commit a violent or dangerous act. Such comments may range from subtle innuendo to direct threats that, when taken in conjunction with other information, paint a more complete picture of the potential for violence.
  - c. A personal history that reflects prior violence under similar or related circumstances. The person's history may be known to the officer, the family, friends, or neighbors, who may be able to provide such information.
  - d. Failure to act prior to arrival of the officer does not guarantee that there is no danger, but it does tend to diminish the potential for danger.

- e. The amount of control that the person demonstrates is significant, particularly the amount of physical control over emotions of rage, anger, fright, or agitation. Signs of a lack of control include extreme agitation, the inability to sit still or to communicate effectively, wide eyes, and rambling thoughts and speech. Clutching one's self or other objects to maintain control, begging to be left alone, or offering frantic assurances that one is all right may also suggest that the individual is close to losing control.
- f. The volatility of the environment is a particularly relevant factor that officers must evaluate. The surroundings should be kept as calm as possible. Any elements that agitate the environment, or that make for a particularly combustible environment, or that may incite violence should be considered.

#### **IV. APPROACH AND INTERACTION – General Guidelines**

- A. The following general guidelines detail how to approach and interact with a person who may have a mental illness and who may be a crime victim, witness, or suspect. These guidelines should be followed in all contacts, whether on the street or during more formal interviews and interrogations. Officers, while protecting their own safety, the safety of the person with mental illnesses, and others at the scene should do the following:
  - 1. Recognize that these events are dangerous, and officers must be prepared to protect themselves and others. The person may be suffering from mental instability, extreme emotions, paranoia, delusion, hallucinations, or intoxication.
  - 2. Remain calm and avoid overreacting. Surprise may elicit a physical response, or the person's "fight or flight" may be engaged.
  - 3. Approach the individual from the front.
  - 4. Be helpful and professional.
  - 5. Provide or obtain on-scene emergency aid when treatment of an injury is urgent.
  - 6. Check for and follow procedures indicated on medical alert bracelets or necklaces.
  - 7. Indicate a willingness to understand and help. Use active listening, and paraphrase responses.
  - 8. Use the person's name and your name when possible.
  - 9. Speak slowly, simply, and briefly.
  - 10. Move slowly.
  - 11. Remove distractions, upsetting influences, and disruptive people from the scene.
  - 12. Understand that a rational discussion may not take place.

13. Recognize that sensations, hallucinations, thoughts, frightening beliefs, sounds (“voices”), or the environment are “real” to the person and may overwhelm the person.
  14. Be friendly, patient, accepting, and encouraging, but remain firm and professional.
  15. Be aware that your uniform, gun, and/or handcuffs may frighten the person with mental illnesses. Reassure him or her that no harm is intended.
  16. Attempt to determine if the person is taking any psychotropic medications.
  17. Announce actions before initiating them.
  18. Gather information from family or bystanders.
  19. Use patience and communications to control.
  20. Use physical force only as a last resort.
  21. Don’t be afraid to ask direct questions about what the person is experiencing, such as, “Are you hearing voices? Are you thinking of hurting yourself? Are you in need of something?”
- B. Officers should be aware that their own actions might have an adverse effect on any situation that involves a mentally ill person. Actions that officers should generally avoid include the following:
1. Moving suddenly, startling the person, giving rapid orders, or shouting.
  2. Forcing discussion.
  3. Cornering or rushing.
  4. Touching the person (unless essential for the safety of the person, bystanders, or the officer involved).
  5. Crowding the person or moving into his or her zone of comfort.
  6. Expressing anger, impatience, or irritation.
  7. Assuming a person who does not respond cannot hear.
  8. Using inflammatory language, such as “mental” or “mental subject.”
  9. Challenging delusional or hallucinatory statements.
  10. Misleading the person to believe that officers on the scene think or feel the way the person does.

- C. The department shall provide training to all department personnel. This training shall be provided to all newly hired personnel during their first year of employment, with refresher training given to all personnel at least every three (3) years.

## **V. EMERGENCY APPREHENSION AND DETENTION**

- A. HSC 571.003 defines "mental illness" as an illness, disease, or condition, other than epilepsy, senility, alcoholism, or mental deficiency, that has the following effects:
1. Substantially impairs a person's thought, perception of reality, emotional processes, or judgment; or
  2. Grossly impairs behavior as demonstrated by recent disturbed behavior.
  3. HSC 573.001 empowers peace officers without a warrant to take into custody a person if the officer has reason to believe and does believe the following:
    - a. the person is mentally ill; and
    - b. because of that mental illness there is a substantial risk of serious harm to the person or to others unless the person is immediately restrained; and
    - c. believes that there is not sufficient time to obtain a warrant before taking the person into custody.
  4. A substantial risk of serious harm to the person or others under Subsection (a)(1)(B) may be demonstrated by the following:
    - a. the person's behavior; or
    - b. evidence of severe emotional distress and deterioration in the person's mental condition to the extent that the person cannot remain at liberty.
  5. The peace officer may form the belief that the person meets the criteria for apprehension based on the following:
    - a. representation of a credible person.
    - b. the conduct of the apprehended person.
    - c. the circumstances under which the apprehended person is found.
  6. A peace officer who takes a person into custody shall immediately transport the apprehended person to:
    - a. the nearest appropriate inpatient mental health facility; or
    - b. a mental health facility deemed suitable by the local mental health authority if an appropriate inpatient mental health facility is not available.

7. A jail or similar detention facility may not be deemed suitable except in an extreme emergency.
8. A person detained in a jail or a non-medical facility shall be kept separate from any person who is charged with or convicted of a crime.

B. Juvenile Mentally Ill Patients: Emergency detention procedure for juveniles is the same as for adults.

## **VI. TAKING A PERSON INTO CUSTODY FOR EMERGENCY DETENTION**

A. If an officer determines that an emergency detention is necessary, the following procedures will be utilized:

1. A minimum of two officers should be present before any action is begun toward taking the subject into custody.
2. An officer who feels that a patient should be taken into custody will not force entry into the home of the mentally ill person unless a life is in immediate danger.
3. The officers taking the person into custody will apply handcuffs for transport. The officers should explain that handcuffs are necessary for everyone's protection. They should use front cuff with belt restraint if possible. Officers who believe the subject will not resist should inform the subject of their intentions beforehand and explain their reasoning. Officers who believe the subject will resist should understand that immediate forceful action may be necessary to restrain the individual. Officer safety is paramount.
4. Officers are reminded that the use of force is authorized to the extent necessary to take the subject into custody.
5. The officers should proceed to the mental health facility and turn the subject over to the staff.
6. The officers must complete an "Notification of Emergency Detention" form, which details actions of the subject that led the officer to believe there was danger to the subject or to others.
7. The officer must complete an incident report detailing the event and attach a copy of the "Notification of Emergency Detention" form to the report.

B. Physically Ill Mentally Disturbed Persons. When a mentally ill person is also physically ill or injured so that transport by ambulance is necessary, an officer will follow the ambulance to the nearest health care facility.

## **VII. CRIMINAL OFFENSES INVOLVING THE MENTALLY ILL**

- A. If an officer believes that an individual who commits a crime is exhibiting symptoms of mental illness and the person is an immediate danger to himself/herself or others, the officer should apprehend the person and take him/her to a mental health facility under an “Notification of Emergency Detention”. The officer will prepare an offense report that provides all the details of the offence and a description of the subject’s behavior. If an evaluation determines that the individual is competent, he/she will be filed on for the offense and an arrest warrant obtained.
- B. Individuals who commit criminal acts and are believed by the officer to be exhibiting symptoms of mental illness but there is no evidence that the person is an immediate danger to themselves or others should be treated as follows:
  - 1. If the offense is a misdemeanor, release to a competent adult caregiver or booked into jail. If booked into jail, every attempt will be made to locate a caregiver and release the person to the caregiver, if agreed upon with the magistrate. In such cases a PR Bond should be recommended to the magistrate.
  - 2. If the offense is a felony, the individual will be booked into jail and every attempt will be made to contact a caregiver. The individual will be required to make bond.
  - 3. In cases of family violence, a supervisor or the Chief of Police should be consulted to determine an appropriate response.
  - 4. In any case involving a person in which the officer suspects they are mentally ill is booked into jail, but not housed with other inmates in accordance with the county jail policies and procedures. Every effort will be made to monitor that person’s safety. Process the individual as quickly as possible to remove him/her from the facility.
  - 5. Juveniles who are suspected of being mentally ill but non-violent who are being cared for by a responsible person will not be detained unless a felony has been committed.
  - 6. Violent juveniles who are suspected of being mentally ill or those who have committed a felony will be transported to the mental health facility.

## **VIII. REPORTING**

- A. If a criminal incident involving a mentally ill person is reported, all pertinent information involving the offense must be included in that report.
- B. Certain individuals may habitually display unusual behavior that is or may become well known to the police department. Whenever contact is made with these individuals, a Field Interview (FI) card should be completed.
- C. Information that is included in the computer-aided dispatch (CAD) regarding a mentally ill person who is a hazard to police officers should be written up by a supervisor and sent to the communications supervisor.

## **IX. REFERRALS TO MENTAL HEALTH FACILITIES**

- A. When a police employee receives a telephone call from a person who appears to be mentally disturbed or irrational, the employee should proceed as follows:
1. Obtain the caller's name, telephone number, and address or the location from which the individual is calling.
  2. If the caller indicates that any life, including the caller's, may be in danger, an officer will be sent, and a supervisor advised of the situation.
  3. If the caller is not an immediate threat to themselves or others, the employee may suggest that the caller contact a local mental health center for assistance.
  4. When an officer is dispatched to a call in which a person has attempted suicide or is threatening suicide, the officer shall make certain that the immediate situation is stabilized. The officer shall also attempt to locate a relative, close friend, or other responsible party who is available. The officer shall then contact the appropriate mental health facility/provider for assistance and/or emergency detention. An incident report shall be completed regarding the attempted suicide.



Notification--Emergency Detention NO. \_\_\_\_\_

DATE: \_\_\_\_\_ TIME: \_\_\_\_\_

THE STATE OF TEXAS  
FOR THE BEST INTEREST AND PROTECTION OF:

\_\_\_\_\_

NOTIFICATION OF EMERGENCY DETENTION

Now comes \_\_\_\_\_, a peace officer with Teague Police Department, Freestone County, of the State of Texas, and states as follows:

1. I have reason to believe and do believe that (name of person to be detained) \_\_\_\_\_ evidences mental illness.

2. I have reason to believe and do believe that the above-named person evidences a substantial risk of serious harm to himself/herself or others based upon the following:

\_\_\_\_\_  
\_\_\_\_\_

3. I have reason to believe and do believe that the above risk of harm is imminent unless the above-named person is immediately restrained.

4. My beliefs are based upon the following recent behavior, overt acts, attempts, statements, or threats observed by me or reliably reported to me:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

5. The names, addresses, and relationship to the above-named person of those persons who reported or observed recent behavior, acts, attempts, statements, or threats of the above-named person are (if applicable):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_


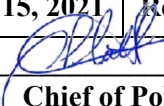
For the above reasons, I present this notification to seek temporary admission to the (name of facility) \_\_\_\_\_ inpatient mental health facility or hospital facility for the detention of (name of person to be detained) \_\_\_\_\_ on an emergency basis.

6. Was the person restrained in any way? Yes  No

\_\_\_\_\_  
PEACE OFFICER'S SIGNATURE

BADGE NO. \_\_\_\_\_

Address: 315 Main Street Teague, Texas Zip Code: 75860  
Telephone: (254) 739-2553

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 8.3 Assisting the Developmentally Disabled</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b>	

**I. POLICY**

Persons afflicted with developmental disabilities are limited in their ability to effectively communicate, interact with others, and make reasoned decisions on their own. While the symptoms may appear like individuals with mental illness, the reason for their behavior is different. Therefore, it is the policy of this agency that officers understand the symptomatic behavior of such persons and be prepared to deal with them in a manner that will best serve their needs and the needs of this department and the community as a whole.

**II. PURPOSE**

It is the purpose of this policy to provide officers with information on the symptoms and effects of developmental disabilities so that officers may better recognize and deal with such persons in enforcement and related capacities.

**III. DEFINITION**

**Developmental Disability:** A potentially severe, chronic disability attributable to a physical or mental impairment or combination of impairments resulting in substantial functional limitations to major life activities, such as understanding and speaking, learning, mobility, self-direction, self-care, capacity for independent living, and economic self-sufficiency.

Developmental disabilities -- such as developmental delays, autism, or Tourette's syndrome - - are not the same as and should not be confused with forms of mental illness, such as schizophrenia or the more common mood disorders.

Many of the symptoms of a developmental disability resemble the symptoms of mental illness. However, they are quite distinct in origin. A developmental disability is one that has slowed or halted an individual's normal development. The result may be permanent. Mental illness may occur in individuals who have fully developed mentally and physically but whose illnesses impact their behavior.

## IV. PROCEDURES

A. Common Symptoms. Developmental disabilities take many forms. Also, many of the persons who have such disabilities have other related but distinct disorders as well, such as Asperger syndrome, Fragile X syndrome, and Rett syndrome. Although officers are not able to diagnose persons with such disabilities, officers shall be alert to the symptoms that are suggestive of such disorders. These include but are not limited to the following symptoms in various combinations and degrees of severity:

1. Difficulty communicating and expressing oneself.
2. Communication by pointing or gesturing rather than words.
3. Repetition of phrases or words.
4. Repetitive body movements some of which may be harmful to themselves. These movements may include, but are not limited to, swaying, spinning, clapping hands, flailing arms, snapping fingers, biting wrists, or banging the head.
5. Little or no eye contact.
6. Tendency to show distress, laugh, or cry for no apparent reason.
7. Uneven or gross movements with poor fine motor skills.
8. Unresponsiveness to verbal commands; appearance of being deaf even though hearing is normal.
9. Aversion to touch, loud noise, bright lights, and commotion.
10. No real fear of danger.
11. Oversensitivity or under sensitivity to pain.
12. Self-injurious behavior.

B. Common Encounters. Officers may encounter persons who have developmental disabilities in a variety of situations many of which involve persons without such disabilities. However, due to the nature of developmental disabilities, it is possible to identify some of the most common situations in which such persons may be encountered.

1. Wandering. Developmentally delayed, autistic, or other developmentally disabled persons sometimes evade their parents, supervisor, caregiver, or institutional setting and may be found wandering aimlessly or engaged in repetitive or bizarre behavior in public places, such as stores or on the street.
2. Seizures. Some developmentally disabled persons, such as those suffering from autism, are subject to seizures, and may be encountered by police in response to a medical emergency.

3. Disturbances. Disturbances may develop and a caregiver may be unable to maintain control of the disabled person who is having a tantrum or engaging in self-destructive or threatening behavior.
  4. Strange and bizarre behavior. Strange or bizarre behavior may take innumerable forms, such as picking up items in stores (perceived shoplifting), repetitive and seemingly nonsensical motions and actions in public places, inappropriate laughing or crying, and personal endangerment.
  5. Offensive or suspicious persons. Socially inappropriate or unacceptable acts, such as violation of personal space, annoying others, or inappropriate touching of others or oneself, are sometimes associated with the developmentally disabled who often are not aware of what constitutes acceptable social behavior.
- C. Handling and De-escalating Encounters. Some persons with developmental disabilities can be easily upset and may engage in tantrums or self-destructive behavior. They may become aggressive. Fear, frustration, and minor changes in their daily routines and surroundings may trigger such behavior. Therefore, officers shall take measures to prevent such reactions and de-escalate situations involving such persons while taking enforcement and related actions. These include the following:
1. Speak calmly; use nonthreatening body language, with your hands to your sides. Using a stern, loud, command tone to gain compliance will have either no effect or a negative effect on a developmentally disabled person. Be aware that such persons may not understand the Miranda warning even if they say they do.
  2. Keep the commotion down. To the degree possible, eliminate loud sounds, bright lights, and other sources of overstimulation. Turn off sirens and flashers, ask others to move away, or, if possible, move the developmentally disabled person to more peaceful surroundings.
  3. Keep animals away. Keep canines in the police vehicle and preferably away from the area and ensure that other dogs are removed.
  4. Look for personal identification. Look for medical ID tags on wrists, neck, shoes, belt, or other apparel. Some persons carry a card noting that they are developmentally disabled and possibly nonverbal. That card should also provide a contact name and telephone number.
  5. Call the contact person or caregiver. The person's caregiver or institutional or group home worker is an officer's best resource for specific advice on calming the person and ensuring the safety of the person and the officer until the contact person arrives on the scene.
  6. Prepare for a potentially long encounter. Dealings with such a person should not be rushed unless there is an emergency situation. De-escalation of the situation, using calming communication techniques, can take time, and officers should inform their dispatcher or supervisor or both that this might be the case if circumstances dictate.


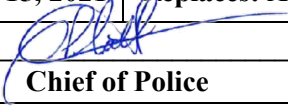
7. Repeat short, direct phrases in a calm voice. For example, rather than saying, "Let's go over to my car where we can talk," simply repeat "Come here," while pointing until the person's attention and compliance are obtained. Gaining eye contact in this and related situations is essential but may be difficult. Be direct by repeating, "Look at me," while pointing to the person's eyes and yours.
8. Be attentive to sensory impairments. Many persons who have autism or other developmental disabilities may have impairments that make it difficult for them to process incoming sensory information properly. For example, some may experience buzzing or humming in their ears that makes it difficult for them to hear. An officer who identifies a sensory impairment should take precautions to avoid exacerbating the situation.
  - a. Do not touch the person. Unless the person is in an emergency (e.g., has been seriously injured or is in imminent peril), speak with the person quietly and in a nonthreatening manner to gain compliance.
  - b. Use soft gestures. When asking the person to do something, such as look at you, speak and gesture softly. Avoid abrupt movements or actions.
  - c. Use direct and simple language. Slang and common officer expressions (e.g., "spread 'em") have little or no meaning to such persons. Normally, they will understand only the simplest and most direct language (e.g., come, sit, stand).
  - d. Do not interpret odd behavior as belligerent. In a tense or even unfamiliar situation, these persons will tend to shut down and close off unwelcome stimuli. For example, they may cover their ears or eyes, lie down, shake or rock, repeat questions, sing, hum, make noises, or repeat information in a robotic way. This behavior is a protective mechanism for dealing with troubling or frightening situations. Do not stop this repetitive behavior unless it is harmful to the individual or others.
  - e. Be aware of different forms of communication. Some developmentally disabled persons carry a book of universal communication icons. Pointing to one or more of these icons will allow these persons to communicate where they live, their mother's or father's name, address, or what he or she may want. Those with communication difficulties may also demonstrate limited speaking capabilities, at times incorrectly using words such as "you" when they mean "I."
  - f. Do not get angry at antisocial behaviors. For example, when asked a simple question, such as "Are you all right?" the person may scream, "I'm fine!" Many such persons do not understand that this is not appropriate.
  - g. Maintain a safe distance. Provide the person with a zone of comfort that will also serve as a buffer for officer safety.

D. Taking Persons into Custody. Taking custody of a developmentally disabled person should be avoided whenever possible as it will invariably initiate a severe anxiety response and escalate the situation. Therefore, in minor offense situations, officers shall explain the circumstances to the complainant and request that alternative means be taken to remedy the situation. This normally will involve release of the person to an authorized caregiver. In more serious offense situations or where alternatives to arrest are not permissible, officers shall observe the following guidelines:

1. Contact a supervisor for advice.
2. Avoid the use of handcuffs and other restraints unless necessary. Use of restraints will invariably escalate panic and resistance.
3. Summon the person's caregiver to accompany the person and to assist in the calming and intervention process. If a caregiver is not readily available, summon a mental health crisis intervention worker if available.
4. Employ calming and reassuring language and de-escalation protocols provided in this policy.
5. Do not incarcerate the person in a lockup or other holding cell unless necessary.
6. Do not incarcerate the person with others.
7. Until alternative arrangements can be made, put the person in a quiet room with subdued lighting with a caregiver or other responsible individual or an officer who has experience in dealing with such persons. Provide the person with any comfort items that may have been in his or her possession at the time of arrest, such as toys, blankets, foam rubber objects.

E. Interviews and Interrogations. Officers conducting interviews or interrogations of a person who is, or who is suspected of being, developmentally disabled should consult with a mental health professional and the prosecuting attorney's office to determine whether the person is competent to understand his or her rights to remain silent and to have an attorney present. If police interview such persons as suspects, victims, or witnesses, officers should observe the following to obtain valid information:

1. Do not interpret lack of eye contact and strange actions or responses as indications of deceit, deception, or evasion of questions.
2. Use simple, straightforward questions.
3. Do not employ common interrogation techniques, suggest answers, attempt to complete thoughts of persons slow to respond, or pose hypothetical conclusions, recognizing that developmentally disabled persons are easily manipulated and may be highly suggestible.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 8.4 Active Shooter Response</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 6.01, 6.02, 6.07, 7.34, and 8.07	

**I. POLICY**

An active shooter is defined as one or more subjects who participate in a random or systematic homicidal spree by demonstrating their intent to continuously harm others. The subject’s overriding objective appears to be mass murder rather than other criminal conduct, such as robbery or kidnapping.

It is the policy of this agency to respond, contain, and stop the threats and to administer aid to the victims.

**II. PURPOSE**

To establish policy and procedures governing the response and activities associated with an active-shooter event that will mitigate any further risk of injury or death to civilian or law enforcement personnel.

**III. PROCEDURES**

**A. Notifications**

The ranking supervisor or officer will notify the chain of command to include the Chief of Police or his/her designee of any active shooter event. Fire and EMS should be notified and requested to stand by in accordance with their protocols.

**B. Mutual Aid**

Upon arriving at the scene of an active shooter event and after assessing the crime scene, the agency should implement its mutual aid agreements with other police agencies if necessary, and with fire and rescue agencies. Additionally, it may be necessary after the incident to collaborate with recovery agencies to assist with the scene and any victims.

## **IV. ACTIVE SHOOTER RESPONSE**

The first two to five responding officers should form a single team and enter the structure (A single officer entering a structure must understand the inherent risk assumed in taking such an action.). Responding officers should never delay their arrival or deploying preventative tactics to await additional officers' arrival in an active shooter situation. It is paramount to the protection of life that officers arrive rapidly and begin to contain and stop the threat in these situations.

The first officers entering the structure should recognize that their primary objective is to stop further violence. Officers should identify and communicate locations of victims needing medical attention. If practical, and absent continued shooting, officers should treat any massive hemorrhaging that may result in the immediate loss of life.

### **A. Concepts and Principles**

Safe, effective responses to active shooters are designed around concepts and principles. The first responding officers should:

1. Stay together as much as possible and enter the involved structure quickly.
2. Maximize communication by staying in close contact with other first responders.
3. Maximize threat coverage by addressing all angles.
4. Visually search involved areas using 540 degrees of coverage around and above the team.
5. Evaluate rooms from the threshold (commonly referred to as slicing the pie).
6. Differentiate between deliberate and direct-to-threat speeds and use the appropriate speed for the circumstances.
7. Use cover-contact principles when taking suspects into custody.

### **B. Follow-On Responders**

Follow-on responders should be directed to victim locations if there is no active threat. Follow-on responders should:

1. Establish and maintain security in the area that follow-on responders occupy.
2. Consider the involved structure as unsearched.



3. Not enter a hallway unannounced if it is occupied by other officers.
4. Unless what other officers want accomplished is very clear, move to them after notifications and conduct a face-to-face meeting.
5. Direct victims to safety by utilizing either shelter-in-place or evacuation. If evacuating, establish a cordon of first responders to the desired exit point to ensure safety of victims.
6. Establish a casualty collection point (CCP) for injured persons. The CCP should be a room or open area (if outside of the structure) capable of holding all victims with injuries that require medical treatment and afford them protections from further violence. A series of rooms next to each other can be considered if casualties exceed available space.
7. Communicate with all involved responders to ensure the area remains secure while facilitating victim treatment.

### **C. Post-Event**

Responses to an active-shooter event must include the aftermath of the incident. Officers should apply the SIM model (Security / Immediate Action Plan / Medical).


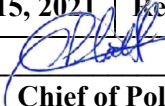
1. Security should take priority. Responding officers must ensure that the immediate environment they are working in remains secure, particularly if the active shooter remains a threat.
2. After officers have addressed known threats, they should formulate an immediate action plan as quickly as possible. This plan should be quick and simple and address: “if / then” – the fluid variables of the situation.
3. Responding officers should address medical issues as soon as they establish security and have an immediate action plan in place.

### **D. OIS Investigations**

Should there be an exchange of gunfire the agency will implement its officer-involved-shooting policy and respond accordingly.

## **V. Media Inquiry**

All requests for information should be funneled through the public information officer (PIO) or the Chief of Police for vetting and coordination. Consideration should be given to establishing a media staging location that is not within the immediate vicinity of the active-shooter event.

	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 9.0 Prisoner Processing</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____ <div style="text-align: center; margin-left: 150px;">   <b>Chief of Police</b> </div>
	<b>Reference:</b> Texas Best Practices 10.10, 10.12, 10.14, 10.15, and 10.22

## I. POLICY

This department does not maintain or operate a holding facility. All persons taken into custody are taken directly to the Freestone County Jail. The policy of this department is to process prisoners without delay and safely transport them to the county jail as soon as possible.

## II. PURPOSE

The purpose of this policy is to provide operational procedures for transport of prisoners to and from the county jail.

## III. GENERAL ISSUES

### A. Supervision

1. The sheriff is responsible for the operational policies and supervision of the county jail.
2. Members of this agency will conform to the county's requirements when processing prisoners for holding in the county's facility.
3. Any difficulties encountered by members of this department should be brought to the attention of a department supervisor as soon as possible.

### B. Access to Facility

1. Access to the county jail is limited to authorized sworn personnel.
2. Juveniles are prohibited from entering the facility at any time.

(Juveniles taken into custody are transported immediately to the juvenile's home, to the juvenile processing room at the police facility, or to the juvenile detention facility only.)

## **IV. FACILITY SECURITY**

### **A. Firearms and Weapons**

1. Firearms and Ammunition are prohibited inside a correctional facility.

(Officers shall secure weapons in an appropriate lock box or in the officer's vehicle trunk prior to entering the facility.)

2. Weapons that are not part of an investigation but are the prisoner's property will be turned over to the booking staff for return to the arrested person on their release.

## **V. PRISONER PROCESSING**

### **A. Prisoner Control and Security**

1. All arrested persons are thoroughly searched for weapons and contraband at the scene of the arrest prior to being placed in a police vehicle.
2. Any contraband located on the arrested person is considered evidence, seized, and properly secured as evidence.
3. Any property removed from a suspect shall be secured by the arresting officer and released to the custody of the county when the individual is booked into the jail. (TEXAS BEST PRACTICES 10.10)
4. Persons arrested by this agency may be transported to the department facility for paperwork processing prior to transport to the county jail.
5. At no time will any person arrested or detained be left alone while in custody, including the police vehicle or the department facility.
6. Persons to be detained in the county jail are escorted into the facility.
7. Upon arrival at the facility, arrested persons are placed into the booking area for intake processing.
8. All booking activity -- including interviews, fingerprinting, photographing, and similar actions -- is conducted by the jail booking staff.
9. Officers will take extra precautions to ensure that all items taken from a prisoner in the field are turned over to the county for safekeeping. (The property is returned to its owner at the appropriate time.)
10. Officers who develop information during an arrest -- through observation or self-profession by the arrestee -- that the individual may be suicidal, is homosexual, transgender, intersexual, or gender nonconforming will make sure that holding facility staff is informed of the situation in a manner that does not embarrass or endanger the arrestee.

## B. Juvenile Detentions

1. Juveniles who are detained and transported to the police building will be held only in the area designated as the juvenile processing office.
2. Under no circumstances will a juvenile in custody be left unsupervised.
3. All juveniles held at the police facility will remain out of sight and sound of adult prisoners.
4. A juvenile who is being held for a status offense is not to be detained in a secured area or any locked room.
5. Status offenders are held in a non-secured area, out of sight and sound of adult prisoners.

## C. Strip Searches (TEXAS BEST PRACTICES: 10.14)

1. Strip searches may be requested when officers have reasonable cause to believe the prisoner(s) may be concealing a weapon, drug, or other contraband or in compliance with the county jail policies and procedures.
2. Strip searches are never performed in the field.
3. A strip search may not be performed until it has been approved by a department supervisor, or in compliance with the county jail policies and procedures regarding intaking of prisoners.
4. A strip search must be performed with the assistance of county personnel in the county jail.
5. Strip searches are conducted in the manner prescribed by county procedures.
6. Strip searches are documented in the officer's arrest report, which will detail the officer's justification for such a search, the approving supervisor's name, the location where the each took place, the names of all persons present during the search, and the results of the search. A copy of the report is forwarded to the Chief of Police for review and filing.

## D. Body Cavity Searches (TEXAS BEST PRACTICES: 10.15)

1. Body cavity searches are never performed in the field and, if requested and approved, are conducted only by competent medical personnel in compliance with county procedures.
2. If an officer has reasonable cause to believe a body cavity search is needed to detect weapons, drugs, or other contraband, the following procedures apply:

- a. A supervisor is notified.
- b. A search warrant is secured.
- c. The detainee is transported to an appropriate medical facility.
- d. The search is conducted by the on-duty emergency room physician while officers stand by to take control of any evidence and provide security to the physician conducting the search.
- e. Body cavity searches are documented in the officer's arrest report and will detail the officer's justification for such search, the approving supervisor's name, the identity and the location of the facility where the search took place, the names of all persons present during the search, and the results of the search. A copy of the search warrant application, search warrant, and inventory shall be attached with the officer's report.
- f. A copy of the report and of the warrant are forwarded to the Chief of Police for review and filing.

E. Medical Attention (TEXAS BEST PRACTICES: 10.12)

1. Should an arrested person have obvious injuries or complain of injury or illness, the arresting officer will ensure the individual is examined by either EMS personnel or medical personnel before transport to the county jail.
2. If the severity of medical conditions is unclear or if a prisoner requests medical attention, he/she shall be transported as soon as possible to a medical facility for evaluation.
3. If necessary, for medical treatment, Emergency Medical Services (EMS) shall be responsible for transporting the prisoner to the designated medical facility. The arresting officer will follow EMS to the designated medical facility unless other arrangements have been made. The arresting officer shall provide for the security of the prisoner while at a designated medical care facility. Officers should avoid transporting persons requiring medical treatment unless they are near the medical center and EMS response would significantly delay appropriate medical treatment.

F. Fingerprints and Photographs

1. Individuals being charged with a class B misdemeanor or above require the state issued CJIS card and any supplemental cards as required.
2. Those individuals being charged with a felony also require both a CJIS card and an FBI card.
3. Fingerprinting is not required for those being charged with a class C misdemeanor; however, fingerprints may be taken if, in the opinion of the booking officer, they would be useful in fully identifying the arrested person or is part of the county jail's policies and procedures.

4. All adult individuals detained will have a booking photo made.

#### G. Arrest Reports

1. Using the Freestone County Arrest report, the arresting officer will complete an arrest report for every individual detained.
2. Arrest reports must contain information about the offense and the probable cause to believe the person committed the offense or a reference to an offense report where such information is provided.
3. All arrest reports and related offense reports will be completed by the arresting officer and provided to county jail personnel.

#### H. Receiving Prisoners from Other Agencies

1. Prior to accepting prisoners from other agencies, the receiving officer must have the following:
  - a. Positive identification of the detainee.
  - b. Positive identification of the officer delivering the prisoner.
  - c. Telephonic or written confirmation of the reason for the incarceration, such as a copy of an offense report, an arrest report, a warrant, and bond information if any.
  - d. Assurance that an offense has occurred and that authority for arrest exists.

#### I. Transportation of Prisoner to Other Agencies and Receiving Prisoners from the County

1. Officers transporting prisoners to another agency are responsible for the following:
  - a. Complying with the other agency's rules, which include putting all weapons in a lock box or securing them in the trunk of the officer's vehicle.
  - b. Keeping the prisoner in handcuffs until the other agency accepts custody.
  - c. Providing the receiving agency with all necessary paperwork and the prisoner's property.
2. Officers picking up prisoners from the county will inquire about any physical or mental problems the prisoner may have.
3. An officer who picks up a prisoner from the county will see that the prisoner signs for his/her property.
4. The transporting officer will receive the prisoner's property for safekeeping.  
(TEXAS BEST PRACTICES: 10.10)

## **VI. PRISONER RIGHTS**


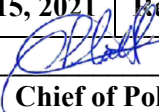
### **A. Access to Consul (TEXAS BEST PRACTICES: 10.22)**

1. Detainees are asked their citizenship. Detainees who are not U.S citizens are asked by the arresting officer if they wish their consul to be notified. If so, the Consul is notified with information taken from the list of Consuls maintained by the agency.
2. Notification or refusal is noted in the arrest report.

### **B. DWI Blood Tests**

1. Suspects arrested for DWI have the right to request a blood test by a physician of their choice within two hours after their arrest per TRC 724.019.
2. The individual making such a request should be allowed access to a telephone for this purpose as soon as possible.



	<b>TEAGUE POLICE DEPARTMENT</b>
	<b>Policy 10.0 Municipal Court Operations</b>
	<b>Effective Date: November 15, 2021</b>   <b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____ <div style="text-align: center; margin-left: 150px;">   <b>Chief of Police</b> </div>
	<b>Reference:</b> Texas Best Practices 11.01, 11.02, and 11.03

**I. POLICY**

Proper security and decorum in the municipal court are necessary for the administration of justice and for the protection of court personnel and the public. Regardless of the level of offense, court hearings can be emotionally charged and decorum must be maintained. The department provides officers to serve as bailiffs for the municipal court to ensure the security of the court and the protection of court personnel and visitors. The municipal court has jurisdiction only over Class C misdemeanor offenses. Most of the business conducted relates to traffic offenses.

**II. PURPOSE**

The purpose of this policy is to establish guidelines and procedures for the decorum and security of the municipal court.

**III. ORGANIZATION AND STAFFING**

- A. When the municipal court is in session, the police department is responsible for its security. The department is also responsible for emergency operation plans for incidents that might occur in the court.
- B. An officer is assigned as bailiff when the court is in session. Sergeants will ensure that the bailiff reports for court sessions as required. Only an officer who has been trained in courtroom security and in this policy should serve as bailiff.

**IV. OPERATIONS (TEXAS BEST PRACTICES: 11.01)**

- A. The assigned bailiff, who must attend all sessions of the court unless dismissed by the judge, has the following duties:
  - 1. To see that all defendants, witnesses, and observers are seated prior to the entrance of the officers of the court.
  - 2. To perform opening ceremonies of the court and announce the judge.

3. To enforce the rules of the court (posted at the entrance of each courtroom) and preserve order and decorum while the court is in session.
  4. To maintain proper procedures during jury trials, maintain the security of the jury room, and see to the needs of jurors and witnesses.
- C. During judiciary proceedings, the assigned bailiff may be directed by the presiding judge to place an individual under arrest. Whether or not to use physical restraints for such arrests is at the discretion and direction of the presiding judge or as the situation dictates.
- D. High-risk persons brought to the courtroom may be restrained as directed by the judge. The bailiff carries handcuffs during court sessions. Waist chains and leg irons are available in police department.
- E. The bailiff also ensures the security of the court operations by the following:
1. Conducting daily inspections of the duress alarms, if equipped, prior to the time court convenes.
  2. Conducting daily inspections of the fire equipment.
  3. Conducting a physical inspection of the courtrooms prior to each session and after the last session of each day.
  4. Securing the courtrooms when the courts are not in session.
  5. Being familiar with the daily schedules of each judge in case special security is warranted.
  6. Making a walk-through of the building and assisting with the security of the court clerk's office areas.
- F. Pursuant TPC 46.03 weapons on the premises of the court or court offices is prohibited. Any person violating this provision shall be arrested and charged accordingly. Only sworn law enforcement officers may be armed in the courtroom.

#### **IV. COURT SECURITY PLAN**

- A. Facilities and equipment (TEXAS BEST PRACTICES: 11.02)
1. The municipal court judge and court clerk have access to a telephone located in the courtroom.
  2. The bailiff is equipped with a portable police radio.
  3. A magnetometer may be obtained from the holding facility in the event its use is anticipated.

4. The bailiff has access to a flashlight in case of a power failure.
  5. A duress alarm may be installed at the judge's bench.
  6. Fire extinguishers and flashlights are maintained in each courtroom, the court clerk's area, and the building lobby.
- B. Pre-session inspection. The bailiff arrives 30 minutes before the court convenes and determines that:
1. The courtroom is free of weapons and contraband.
  2. The duress alarms and telephones are in working order.
  3. Restraining devices are present and concealed.
  4. Emergency doors in the courtroom are free of obstructions.
  5. Lighting is adequate and emergency lights can be activated in the event of a power failure.
  6. All public entrances are open and free of obstructions; and
  7. All communications equipment is in working order.
- C. Courtroom operations
1. Judges enter and exit the courtroom through the entrance behind the bench.
  2. The public enters and exits the courtrooms only through the main doors leading into the gallery.
  3. Prisoners are brought into or taken out of the courtrooms only after all person's present are seated, or when the courtroom is empty.
  4. The bailiff always remains in the courtroom unless otherwise directed by the judge.
  5. Bailiffs and peace officers are the only persons authorized to carry weapons in the courtroom. If the bailiff believes a person may be carrying a weapon, a hand-held metal detector may be used to conduct a search. A person who refuses a search in this manner must leave the courtroom. During trials, or during periods of security concerns, the judge may request that all persons entering the courtroom be scanned for weapons.
  6. Contraband taken into the courtroom for evidence purposes remains in the possession of the testifying officer unless otherwise directed by the judge.

7. At the discretion of the presiding judge, or at the discretion of the bailiff, briefcases and purses may be searched.

#### D. Unusual occurrences


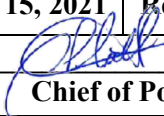
1. In the event of an unusual occurrence, the bailiff or ranking police officer assumes control and requests additional police, fire, or medical assistance as the circumstances require.
2. Medical emergencies in the courtroom
  - a. A first-aid kit is kept in the judge's office and in the bailiff's office.
  - b. All requests for medical assistance or additional security are called in to 9-1-1 or to the dispatch center.
  - c. If the medical emergency involves a person who is in custody, the bailiff maintains security and requests medical assistance and additional police officers.
  - d. If the medical emergency involves a court participant or spectator, the bailiff maintains security of any prisoners that are present and provides any assistance possible. The bailiff contacts the dispatch center via radio (or most appropriate available means) and requests the proper assistance.
  - e. If other police officers are present, the ranking officer assumes control and directs the actions of the bailiff, responding officers, and other personnel.
  - f. The city's volunteer fire department or first responders may provide emergency medical service, until Emergency Medical Service Personnel arrive.
  - g. The bailiff is responsible for all police reports necessitated by a medical emergency.
3. Fire evacuation plan
  - a. Before the court convenes, the bailiff conducts a physical inspection to ensure that all doors are functioning and free of obstructions.
  - b. In the event of a fire in the courtroom or city hall complex, the bailiff assumes control of the courtroom evacuation.
  - c. Those persons present in the courtroom are instructed to exit through the nearest exit door and out the building through the nearest public entrance or exit.
  - d. All calls for fire emergencies are made to 9-1-1 or directly to the dispatch center.

- e. A fire evacuation chart is posted at the rear of the courtroom near the exit.  
(TEXAS BEST PRACTICES: 11.03)
4. Bomb threats
    - a. In the event of a bomb threat, the bailiff notifies police dispatch immediately.
    - b. The bailiff evacuates the court.
    - c. The bailiff ensures that the court administrator is notified of the situation.
  5. Hostage Situations
    - a. The judge sounds the duress alarm, if equipped.
    - b. The bailiff notifies police dispatch, attempts to isolate the actor(s), and, if possible, evacuates and secures the area.
    - c. Field personnel are dispatched to establish and secure a perimeter until arrival of tactical personnel.
  6. High-risk trials
    - a. Persons in custody are not normally brought to the Court Building, and trial defendants are not in police custody; however, if a trial or arraignment should pose a possible threat to the judge, jury, or participants in a proceeding, the judge or prosecutor notifies the bailiff to take additional precautions.
    - b. If the judge deems a trial to be high risk, the bailiff consults with the Chief of Police and assesses the need for further staffing.
  7. Prisoner handling
    - a. All adult prisoners are restrained during the movement to and from the courtroom. For short distances, detainees are handcuffed with hands behind the back until seated in the courtroom. Juveniles are not normally handcuffed unless they present a high risk of injury or extreme aggression.
    - b. Handicapped persons may be restrained as appropriate to the circumstances.
    - c. Once the person is in the courtroom, the bailiff removes the restraints before the jury enters.
    - d. The bailiff replaces the restraints after the jury departs.
    - e. The bailiff maintains a set of handcuffs on his/her person.

- f. Should the prisoner need to be removed from the courtroom, movement is made through the rear entrance near the judge's bench. Or the entrance designated by the court.
- g. All prisoners are searched prior to their court appearance and upon their return to the holding facility.

**V. ANNUAL REVIEW OF COURT OPERATIONS**

- A. An assigned bailiff and the court administrator conduct an annual security inspection of the municipal court facilities. If a structural change in the building occurs, an additional inspection is required. The inspection includes, but is not limited to, the existence, adequacy, and working condition of alarms, communications equipment, fire extinguishers, medical emergency items, emergency light sources, exterior lighting, emergency exits, and the emergency evacuation plan.
- B. The assigned bailiff and court administrator also review the fire evacuation and other emergency operations plans with all court employees. (TEXAS BEST PRACTICES: 11.03)
- C. A copy of the inspection report and description of the training is forwarded to the municipal court judge and the Chief of Police.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 11.0 Property and Evidence Management</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference:</b> Texas Best Practices 12.01, 12.03, 12.04, 12.05, 12.06, 12.07, and 12.08.	

## I. POLICY

Proper documentation, collection, preservation, and submission of physical evidence to forensic laboratories may provide the key to a successful investigation and prosecution. Through evidence located at the scene, suspects are developed or eliminated, investigative leads are established, and theories concerning the crime are substantiated or disproved. The purpose of property and evidence management is to maintain those property items coming into the possession of the department in such a manner as to secure them from theft, loss, or contamination, and to maintain them for easy retrieval as needed.

## II. PURPOSE

The purpose of this policy is to establish property room procedures that will protect the integrity of the property and management system.

## III. ORGANIZATION AND ACCOUNTABILITY

- A. The Chief of Police will appoint a primary and an alternate property custodian. The property custodian is responsible for maintaining security and control of property and evidence that the department acquires through normal duties and responsibilities. The alternate serves as backup when the assigned property custodian is unavailable.
- B. The property custodian reports to Chief of Police.
- C. The property custodian shall satisfactorily complete a TCOLE approved basic course on the management of the property function, on-the-job training, and other related training courses, seminars and/or conferences as appropriate.
- D. Duties Responsibilities

The primary duty of the property custodian is to log, classify, store, dispense, destroy, and release property and evidence to its rightful owner, for court presentation and/or for destruction or auction. Additional duties include but are not limited to the following:

1. Maintain evidence or property in such a manner that the individual items are secure from theft, loss, or contamination, and can be located in a timely manner.

2. Maintain property reports and other documentation associated with the “chain of custody” for all property.
3. Ensure the timely and legally correct notification of owners and release/disposal of property recovered, found, or seized by the Police Services.
4. Operate computer terminals to access information regarding case dispositions and other related information involving the classification and proper disposition of property/evidence.
5. Coordinate the disposal of unclaimed and/or surplus property and the special disposal of narcotics, weapons, explosives, and hazardous materials pursuant to law.
6. Release of property for court, auction, disposal, or person legally entitled to the item.
7. Provide in-service training to department personnel regarding the appropriate logging, packaging, documenting, and storage of property and evidence.
8. Provide effective liaison between the department and local, county, state, and federal law enforcement agencies.
9. Represent the department while attending state and local associations involved with the management of property and evidence.
10. Stay abreast of local, state, and federal law involving property and evidence handling. Recommend and facilitate appropriate changes.
11. Maintain a clean and orderly property storage facility.

#### **IV. FACILITIES SECURITY (TEXAS BEST PRACTICES: 12.04)**

##### **A. Access**

1. The property room is maintained as a secure location. Access to the property room and all other temporary or long-term property storage areas is restricted to the property custodian and the alternate property custodian. All other persons entering the property room will sign in and out on the property room entry log.
2. Other department personnel do not enter property storage areas unless escorted by a property custodian. Except for the property custodians, all Department personnel, visitors, contractors, etc., who enter the property room must sign in and out on the visitor’s log, and the date, duration and purpose of the visit must be noted.
3. Property or evidence is removed from its storage location only by the property custodian or the authorized designee.
4. The doors, gates, or other closure devices to any storage area are secured whenever the property custodian or other authorized personnel is not on the premises.



## B. Key Control

1. Two keys are required to open the main property room doors. The property custodian and alternate are the only individuals with both keys.
2. The keys to all other property storage facilities are kept in the key box located inside the main property room. Both the duplication of keys and the unauthorized possession of keys to secured property storage areas are strictly prohibited.
3. A complete set of other storage facility keys, safe combinations, alarm codes, etc., are in a sealed property envelope, initialed and dated by the property custodians. That envelope stays in the Police Chief's safe as a backup for property room personnel. Inspection of this envelope is part of all property room audits and inventories.
4. Property room personnel may not relinquish property room keys, combinations, or alarm codes to anyone other than authorized personnel.
5. When property custodians leave their assignment, the Chief of Police ensures that all locks, combinations, and codes are changed.
6. New locks are installed if a key is lost, or security is otherwise compromised.

## C. Alarms and Other Security Systems

1. Firearms are stored separately from other property in the property room, secured in the safe or long-gun storage area. The safe always remains locked unless property is being stored, removed, or inventoried.
2. Controlled substances are stored separately from other property in the property room and secured in a safe. That safe always remains locked unless property is being stored, removed, or inventoried.
3. Money is stored separately from other property in the property room and secured in a locked safe. The safe always remains locked unless property is being stored, removed, or inventoried.

## V. CATEGORIES OF PROPERTY

### A. For these procedures, property in police custody falls into these categories:

1. Evidence. Evidence is property that comes into the custody of a police department employee when such property may tend to prove or disprove the commission of a crime, or the identity of a suspect, pursuant to an official criminal investigation. Evidence or assets seized for forfeiture are handled in the same manner as other evidence.

2. Found Property. Found property is property of no evidentiary value that comes into the custody of an agency employee, and whose rightful owner may or may not be known to the finder or the department. Due diligence must be exercised to discover the rightful owner. If the owner cannot be located, the Department will dispose of the property in a time and manner prescribed by law.
3. Safekeeping. Safekeeping is property of no evidentiary value surrendered to an employee of the agency for temporary custody. This arrangement comes with the understanding that the person surrendering the property has the legal right to do so, and that the property will be returned to the rightful owner(s) at the end of a specified period, unless disposition by the Department, in a manner prescribed by law, is requested by the owner(s).

## **VI. DOCUMENTATION AND RECEIPT OF PROPERTY (TEXAS BEST PRACTICES: 12.01)**

### **A. Documentation of Property**

The police employee accepting property writes a report with the following components: (1) a description of the item (2) pertinent details of how the item came into the employee's possession and (3) complete information about the person who found the property, or the person from whom it was seized or recovered.

### **B. Receipt of Property**

The property custodian provides a receipt to any person from whom property is taken regardless of the classification of that property.

### **C. Computer Inquiry and Entry**

1. All employees make the appropriate inquiries to the TCIC on all serialized or identifiable items collected or seized prior to placing the item into storage. This determines if the property has been reported stolen or has been entered into the statewide system for any reason.
2. Dispatch verifies all "hits" before the item is confiscated. After verification, a dispatcher sends the "locate" information.
3. The offense and property report reflects the status of the property items. The report also indicates that a "locate" was sent to the originating agency. It is the originating agency's responsibility to update the TCIC information from "stolen" to "recovered" status.

### **D. Property Forms: The property and evidence function require the use of the following forms:**

1. Evidence Bags and Boxes

- a. Evidence bags and boxes. These serve as the primary method for submitting property for storage. A listing of the case number, date, location, applicable names, description of property, and officer's name and ID number properly identify the property and its origin.
- b. Chain of Custody Form. This form, submitted with each property container (bag, box, etc.), tracks the movement of the item, including its release.
- c. Property Tag. Officers affix a property tag securely to items that do not fit into evidence bags or boxes. This tag designates the case number, date of submission, and name and ID number of the submitting officer.
- d. Money Form. This form serves as the sole method for logging cash money into the property room. Cash is defined as United States coin and currency. Checks, credit cards or other negotiable items do not require the use of a money envelope. The property custodian does not accept money unless it is packaged and logged appropriately, according to the following procedures:
  - i. Itemize money by denomination, listing subtotals and total amounts.
  - ii. All money logged into the property room requires at least two officers or employees to verify the count.
  - iii. All money envelopes must contain at least two signatures verifying the amount listed and enclosed. The entering officer and verifying officer sign their names and numbers to the front of the envelope and seal the envelope with tamper-proof security tape. Both then initial the back of the envelope prior to entering it into the property locker. For accuracy, the officers must conduct two separate counts on large amounts of cash.
  - iv. Extremely large amounts of coin and/or currency seized can be difficult to package in a money envelope, e.g., coins stored in a large piggy bank or bottle, a large amount of bills in a briefcase or satchel. In those rare cases, it is acceptable to log the container and money as is. However, the need for a money count and money form still applies. Officers submitting the money secure the container with evidence tape to prevent tampering and tape the money form to the container.
  - v. Suspected counterfeit bills require a money form but have no cash value. Make a notation on the outside of the money envelope reflecting that the contents contain suspected counterfeit bills.
  - vi. The money form is also used for foreign currency. Officers will indicate on the outside of the envelope that the envelope contains foreign currency.
- e. Property Receipt Form and Property Release Form. The Property Receipt Form serves as a receipt for property taken into custody and documents the release of property to other entities. The Property Release Form also authorizes the release of property. No property is released without a completed Release Form.

## VII. LOGGING PROPERTY AND EVIDENCE

- A. Officers who seize property and can determine ownership in the field may release the property immediately to the owner if the property is not needed for prosecution in a criminal case. Officers should contact the investigating officer or, if necessary, the county attorney's office to determine prosecutorial need. If the property can be released in the field, the officer will complete a Property Release Form and have the owner sign for receipt of the property. The form will be turned in to the property room where the property custodian will enter the property into the system and show that it was released in the field. The Property Release Form will be included in the case file. (TEXAS BEST PRACTICES: 12.06)
- B. Property that is seized by the department and not immediately released to the owner will be entered into the computer system and secured in the property room as soon after seizure as possible. Personal lockers, files, or desks are not approved storage for property or evidence items. Officers will log all property and evidence into the property room before the end of their shift. (TEXAS BEST PRACTICES: 12.03)
- C. Maintaining property/evidence in a case file may be acceptable when it is necessary for the proper investigation of the case by the assigned officer; however, the property/evidence must first be logged into the property system and then signed out. The officer signing out the property /evidence is responsible for the evidence until returning it to the property room. The officer is also responsible for the integrity of the evidence while checked out.
- D. Marking and Packaging
  - 1. All collected property is marked for identification and packaged to avoid contamination.
  - 2. Permanent and distinctive marks, such as initials, ID numbers, and case numbers, should be marked directly on objects collected (when possible) without damaging the evidence.
  - 3. When unable to mark the exhibit itself (such as in the case of stains, hair, blood, controlled substances, etc.), the officer must place the item in a vial, envelope, box, bag or other suitable package, then seal and mark the container as instructed in item 2 above.
  - 4. Containers and materials for use in packaging physical evidence and other property come in a variety of shapes and sizes. Officers strive to use the size and type container appropriate for the type of property. An assortment of packaging materials and supplies for this packaging are near the book-in counter. The property custodian is responsible for maintaining property packaging and storage supplies.
  - 5. Always package FIREARMS, MONEY, AND CONTROLLED SUBSTANCES separately from other property or evidence items. See section C above.

6. Firearms Evidence. The collection of firearms is appropriate for both criminal and non-criminal cases. Due to the very nature of these items, extreme care is taken to ensure the safe handling of all weapons and preservation of their evidentiary value. Weapons are unloaded ONLY after the officer notes the position of the bullets, empty cartridges, safety, bolt, breechblock, hammer, cylinder, magazine, etc.

NOTE: NEVER PLACE A LOADED FIREARM IN AN EVIDENCE STORAGE LOCKER.

Exception: If a weapon cannot be unloaded due to a mechanical defect the officer must attach a warning note to the weapon indicating that it is loaded. The property custodian arranges for the range master (or a qualified designee) to unload the weapon prior to placing it in storage or transporting it to a laboratory. Unfired cartridges may be left in the magazine provided the magazine is removed from the gun.

7. Hazardous Materials / Devices: No unexploded device, or a device that is suspected of being one that might explode, will be transported, or stored in or about the police facility. No Class A explosive, such as dynamite, desensitized nitroglycerin, large quantities of fireworks, or more than one pound of black powder will be transported or stored in or about the police facility.
8. Money: All monies will be itemized by denomination and quantity on the approved money form before it is placed in a property locker. See Section C above.
9. Jewelry: Jewelry items will be packaged individually in an appropriate and suitable container such as an envelope, box, or bag.
10. Bicycles: All bicycles or portions thereof retained by police services are placed into the back area of the police department, inside the building adjacent to the evidence room. Different levels of security for the storage of bicycles may be utilized depending on the property classification of the bicycle (Evidence vs. Found Property).
11. Motor Vehicles: Motor vehicles requiring retention are stored at the City Yard on Magnolia Street or Scott's Collision Center. Small motorized scooters are stored in the fenced property annex area (Magnolia Street). Note: Vehicles may be temporarily stored at the police facility while being processed during a crime scene search. The keys for motor vehicles retained as long-term evidence (homicides, fatal traffic accidents or serious hit-and- runs) remain in the ignition of the vehicle if mechanically feasible. Otherwise, those keys are logged into evidence.
12. License Plates: License plates are the property of the Department of Public Safety (DPS, or appropriate motor vehicle department) from the state of jurisdiction. The public is permitted to use the license plate when the annual fees have been paid. License plates maintained as evidence are logged into evidence. Officers must attempt to return a found license plate to its owner. If that is not feasible, the officer logs the plate into property. The property custodian is then responsible for returning the plate to the owner or DPS.

13. Alcohol: Open containers of alcohol are not logged into the property room. The investigating officer pours out the contents at the scene. The officer then describes the condition of the container and its contents in the police report. Officers avoid booking large quantities of alcoholic beverages into evidence. In rare situations, such as when a sample of the evidence is necessary for prosecution, one unopened container (bottle, can, etc.) is retained, and a photograph of all the evidence is attached to the report. A video is made of the destruction of the remainder and this video is attached to the report or otherwise submitted per department video submission policy.

## **VIII. TEMPORARY STORAGE FACILITIES**

- A. After property is marked for identification and packaged, officers deposit the property into one of the following temporary storage areas:
  1. Metal Storage Lockers: Individual metal property lockers are located evidence processing room. Officers lock the property into one of these lockers. The Evidence custodian has keys to access these lockers.
  2. Large Enclosure: All bicycles, large items, or parts thereof, are temporarily stored in the large enclosure on the east side of the evidence room.
  3. Refrigerator/Freezer: A refrigerator and freezer are in the property room. Officers will contact the evidence custodian to have items that require refrigeration placed in the refrigerator or freezer.
  4. Hazardous Materials Storage
    - a. Hazardous Materials are not stored at the police department, rather they are documented and properly disposed of pursuant appropriate EPA guidelines.
    - b. Fireworks are not stored, but instead photographed. Officers destroy all confiscated fireworks by drowning and physical destruction in view of a video recording device.

## **IX. PROPERTY ROOM COLLECTION, INVENTORY & STORAGE**

- A. Property Collection
  1. Daily, the property custodian or alternate inspects all temporary storage lockers, bins, and annexes to remove and process all property items.
  2. The property custodian or alternate also completes the following:
    - a. Assigns a bar code label to each property item submitted, which is generated through the evidence tracking system.
    - b. Makes the appropriate entries into the automated property system,
    - c. Stores each item in the approved locations,

- d. Arranges for transportation to the laboratory for examination as required, and
- e. Arranges for destruction, release to owner, auction, or other authorized disposition as appropriate.

## B. Property Inventory

1. The property custodian accounts for every item submitted into the property system. This process begins at intake.
  - a. The property custodian or alternate compares items listed on the property forms with those found in temporary storage. If any item is missing, the property custodian immediately notifies the Chief of Police. The submitting officer and/or the supervisor then corrects the discrepancy.
  - b. If the property custodian cannot find a missing item(s), he/she enters the item into the “Unable to Locate” (UTL) file and notifies the Chief of Police via email, explaining the circumstances surrounding the missing property. The supervisor forwards a copy of the email to the employee. Property connected to the case will not be processed until the missing material is found or the discrepancy has been corrected.
  - c. The employee is counseled, by their supervisor, on the department counseling form. A copy of the counseling form is forwarded to the Chief of Police for inclusion in the employee’s disciplinary file. Continued violations of this may result in disciplinary action.

## C. Improperly Submitted Property – “Right of Refusal”

1. Officers submit every item into property in a safe and thorough manner consistent with these guidelines and policy.
  - a. The property custodian has the authority to refuse acceptance of any property item submitted in an unsafe, incomplete, or otherwise improper manner as defined in this manual.
  - b. Property room personnel SHALL NOT accept any money, jewelry, or controlled substances if the seal, envelope, packaging, or container has been opened, tampered with, or otherwise improperly submitted.
  - c. The property custodian immediately notifies the submitting officer’s supervisor, who follows up with the submitting officer.
  - d. All personnel shall immediately correct a breach in safety protocol.

## D. Property Storage

The following types of property and evidence are stored separately and according to the listed guidelines. Other miscellaneous types of property may be stored separately as the property custodian determines.

### 1. Firearms

- a. The property custodian stores all firearms in containers (boxes) specifically designed for handgun, rifle, and/or shotgun. Exceptions can be made for those weapons, which, due to size or other considerations, are not compatible for storage in such containers.
- b. The property custodian segregates all firearms from other types of property retained. All firearms, **REGARDLESS OF PROPERTY CLASSIFICATION**, are stored in the weapons safe inside the property room. The safe always remains locked unless property is being stored, removed, inventoried, or inspected. **NEVER** store ammunition with firearms. All ammunition is stored in the ammunition bin.

### 2. Controlled Substances

- a. The property custodian segregates all drugs and narcotics from other types of property retained. All controlled substances, **REGARDLESS OF PROPERTY CLASSIFICATION**, are stored in the narcotics safe inside the property room. The safe always remains locked unless property is being stored, removed, inventoried, or inspected.
- b. Officers count, verify, test, and weigh controlled substances (or suspected controlled substances) prior to sealing them in containers or bags. The officer then weighs the bag and notes "BW" (for bag weight) and the total weight in grams on the outside of the bag. The bag weight is entered in the property description line as "Marijuana BW 13 grams" or similar.
- c. Property custodian only opens sealed containers to facilitate the transportation and/or destruction of the item.
- d. Felony controlled substances are immediately submitted to the Texas Department of Public Safety Crime Lab for analysis. Misdemeanor substances require a letter from the County Attorney's Office for TDPS Crime lab processing.

### 3. Money

- a. The property custodian segregates all money from other types of property retained. All money, **REGARDLESS OF PROPERTY CLASSIFICATION**, is stored in the safe or, if over \$100.00 is deposited with the City Bookkeeper.



- b. The property custodian deposits money (over \$100) with the city bookkeeper either the same or next working day. The property custodian seals the receipt and the Money Form in the original property envelope and returns it to the safe. The property custodian then makes notations in the computer system, showing that the money has been transferred to the cashier.
  - c. The property custodian deposits smaller amounts of money with the city bookkeeper when their cumulative total reaches \$100.00.
  - d. Exception: When the money itself is evidence, subject to forfeiture (drugs), or examination, it remains in the safe until seized money is processed and delivered to the County Attorney's office for disposition. Money delivered to the County Attorney's office requires a receipt denoting the person receiving the money. This receipt will be turned in with the original case report. The custodian will update records to reflect delivery of the money to the County Attorney's Office.
  - e. The property custodian opens sealed containers only to release the money to its rightful owner or to transfer the money to a financial institution. At least one other police employee is present when opening any money envelope.
  - f. The property custodian secures negotiable stocks, bonds, or bank securities in the safe with other money items. He/she assigns no value to the securities for purposes of showing a recovery value.
4. Homicides
- a. The property custodian stores all items of evidence associated with a given homicide case together, unless that evidence requires storage elsewhere for additional security, safety, or preservation measures.
  - b. Property associated with all homicide cases remain segregated from other types of property retained by the Department.
5. Hazardous Materials
- The property custodian will not keep hazardous materials.
6. Photographs
- a. If 35 mm, or other similar type film is utilized for a criminal case, the property custodian stores undeveloped film canisters separate from other types of evidence the department retains.
  - b. Upon an officer's request, the property custodian transports film and negatives to a private vendor for processing.

- c. The officer submits a Property Form and enters the prints into evidence. A set of prints remains with other items associated with the case. The officer may retain a separate set of prints as a working copy during follow-up. After finishing, the officer forwards the prints to the district attorney as a part of the case file or destroys them.

## 7. Property Management.

Nothing in this manual prevents the property custodian from organizing property as deemed necessary for the efficient operation of the property function.

## E. Computer Entries: Computerized Property System

The property custodian enters all incoming property into the computerized property system as soon as possible. Information entered in this system includes the following:

1. Classification of property
2. Type/description of property
3. Quantity
4. Case number
5. Officer submitting property
6. Location property stored
7. Chain of evidence

## F. Disposition of Property

1. The property custodian updates the status of all property retained in inventory, as necessary.
2. The property custodian retains a complete “hard copy” file on each piece of property as a back up to this computer system. The backup files facilitate regular inspections, audits, and inventories.
3. TCIC / NCIC
  - a. Upon request, dispatch personnel check property items with serial numbers in the TCIC/NCIC system.
  - b. In all cases when releasing a firearm, detectives conduct a criminal history check of the person receiving the weapon. This establishes whether restrictions exist that prevent the release of the firearm to that individual. Additionally, detectives request a “stolen” check through TCIC/NCIC to confirm the status of the firearm.

## G. Electronically stored Evidence (TEXAS BEST PRACTICES 12.08)

1. Video/audio recordings captured by in-car camera and/or body camera (or any other audio/visual camera source) that is determined to be evidence in a criminal case will be stored on the secure police department server.
2. Officers will download these recordings into the password protected records management system and document their actions in the case report.
3. Only authorized personnel will have access to these recordings.
4. A copy of all recordings is also burned to a disk and included with the case report.

## X. PROPERTY AND EVIDENCE RELEASE GUIDELINES

### A. Persons Authorized to Release Property

1. The following persons may authorize the release of property under the provisions of this manual:
  - a. The investigating officer, or the officer's supervisor,
  - b. The Chief of Police,
  - c. A magistrate,
  - d. The county attorney's office
  - e. In cases of found property and property impounded for safekeeping, the impounding officer.

### B. Release Authority

1. A court order is required for the release or disposal of property seized pursuant to a search warrant as well as for any property the ownership of which is contested.
2. Court action involving all suspects must be final and the district attorney's Office must approve the release.
3. All evidence or property collected in homicide cases is stored until the death of the defendant(s) or 99 years from the date of the incident.
4. The Chief of Police may authorize the property custodian dispos of property on no-lead cases after the statute of limitations is past. The statute of limitations for felonies is as follows:
  - a. No limit: murder, manslaughter, FSRA with death

- b. 10 years: theft of estate by administrator, theft by public servant, forgery, indecency with a child, injury to a child, sexual assault
  - c. 7 years: misapplication of fiduciary property
  - d. 5 years: burglary, theft, robbery, arson, kidnapping, abandoning a child
  - e. 3 years: all other felonies.
- 5. The Chief of Police signs approval of evidence destruction on no-lead misdemeanor cases after two years from the commission of the offense.
  - 6. The county attorney approves of property disposed of or released purely in the interest of justice when the statute of limitations has not expired. This applies to any felony or misdemeanor cases.
  - 7. The property custodian retains any property requested for civil litigation until its release is approved by the Chief of Police. The Chief of Police contacts the city attorney prior to disposal of property cases where the city is party to civil litigation.

### C. Disposition Instructions (non-evidence)

#### 1. Found Property

- a. The investigating officer attempts to determine and contact the owner(s) of found property. Officers call that person instructing them to contact the property custodian to schedule an appointment and claim their property.
- b. The owner has 90 days to establish ownership and claim the property.
- c. Exceptions: If sufficient evidence exists to file an asset forfeiture case, funds likely coming from illegal activity are retained. Also, if the owner claiming a firearm is not legally entitled to a weapon under the provisions of the law, or is prohibited from possessing a weapon, the Chief of Police determines the type of release or destruction of the firearm.
- d. Pursuant to Code of Criminal Procedure Art. 18.17, any found property having a value of \$500 or more and the owner is unknown will be advertised as “found” in a newspaper of general circulation prior to forfeiture to the city or destruction.
- e. The property custodian processes all unclaimed property for auction, disposal, or transfer for departmental use.

#### 2. Safekeeping

- a. The property custodian returns property held for safekeeping upon the request of the legal owner or by legal mandate. The property custodian disposes of unclaimed property after 90 days.

- b. Prior to release of firearms, the property custodian requests a criminal history check on the owner or person who intends to pick up the weapon.
- c. The Chief of Police determines the disposition on firearms if the owner is not legally entitled to the weapon or is prohibited from possessing a weapon.
- d. The property custodian requests a TCIC/NCIC “stolen” check on the firearm prior to release.
  - i. If the firearm is stolen, an attempt is made to return it to the rightful owner.
  - ii. If the owner cannot be found, the weapon is destroyed per court order.
- e. When releasing a weapon to the owner, the owner presents a photo ID and provides proof of ownership, if requested. The owner must sign the property release form.
- f. All other types of property held for safekeeping are returned to the owner as soon as possible.

D. Non-Essential Property/Evidence:

- 1. With the concurrence of the county attorney, property that is not essential to a prosecution or future prosecution is released to the owner as follows:
  - a. Property that has no market or investigative value as determined by the county attorney may be destroyed upon completion of the investigation with the county attorney’s permission. Examples include, e.g., glass fragments, or a mutilated bullet not suitable for comparison purposes.
  - b. Property held as evidence but not introduced during the trial is released to the owner upon receipt of a court disposition, provided the prescribed time for appeal has elapsed. In misdemeanor and felony cases, 90 days is the time allowed for an appeal.
  - c. In all cases, the person who receives the property must present a photo ID and sign the property receipt.

E. Court Releases

Officers needing evidence or property for court presentation complete a property release form and have the form signed by a supervisor. The form indicates "temporary release" for court. The officer gives the form to the property custodian, who then completes the chain-of-custody form and releases the item to the officer. In all cases, the person receiving the property must present a photo ID and sign the property receipt.

## **XI. INTERIM RELEASE OF PROPERTY GUIDELINES**

- A. To facilitate the need for officers to remove evidence temporarily from the property room for further investigation, examination, court, etc., the following procedures are established:
1. The officer completes a property release form, has it signed by a supervisor who ensures appropriate need, and forwards it to the property custodian at least 24 hours in advance when possible, weekends and holidays excluded.
  2. If exigent circumstances exist, property may be released to the officer with less prior notification.
  3. Officers checking out evidence for court sign and date the chain-of-custody form for all evidence released.
  4. Officers return all evidence to the property room promptly unless that evidence is held by the court.
  5. Officers repackage or reseal evidence as necessary to ensure the integrity of the item. When evidence is placed in a new evidence bag, the old evidence bag is placed in the new bag along with the evidence, and with the chain- of-custody form on the old bag visible.
  6. Officers will obtain a receipt for property if evidence is turned over to any other agency. The receipt for property shall be returned to the evidence custodian and properly documented in the evidence file system.
- B. The property custodian tracks evidence checked out for court and its return. After 72 hours, notification is given to the officer who has not returned the property.

## **XII. DISPOSAL GUIDELINES (TEXAS BEST PRACTICES: 12.05)**

- A. Disposal of items held in the property room is made in a manner authorized by statute and as provided in policy.
- B. The property custodian disposes of no property item until receiving a release authorization from the assigned officer, Sergeant, Chief of Police, a court order, or written instruction from the county attorney's office.
- C. Upon receipt of a court order, the property custodian disposes of property in the manner indicated in that order.
- D. Property to be destroyed is disposed of in the following ways:
1. Property of little or no auction value is disposed of in an appropriate trash receptacle except as otherwise directed below:
    - a. Papers of a sensitive nature will be shredded.

- b. The contents of open alcoholic beverage containers are poured down the drain before the container is disposed of in the trash.
  - c. Property of value (except firearms, money, ammunition, controlled substances, and hazardous materials) is sold at auction, destroyed, or designated for department use.
  - d. Firearms may be converted to department use (if appropriate and approved through the established legal process) or are destroyed.
  - e. Ammunition is disposed of through pre-approved, designated agencies or designated for department use. (See section 2, below.)
  - f. Controlled substances are burned or otherwise disposed of as hazardous waste material. (See section 2 below.)
  - g. Hazardous materials are disposed of through an authorized, pre-approved hazardous waste disposal firm.
  - h. Knives, clubs, BB or pellet guns, or other dangerous weapons are destroyed in the same manner as firearms.
  - i. All unclaimed money is deposited in the City of Teague general fund, except rare coins or rare paper money that will be sold at public auction.
2. Disposition of Firearms

All firearms will be destroyed unless released to their rightful owner with three exceptions.

- a. Firearms that are scheduled for disposal that could be used by the department may be converted to departmental use upon written approval of the city administrator or court order. These weapons will become the property of the department and not individual officers and will be tracked and accounted for on inventories and audits.
  - b. Weapons of intrinsic collectable value or long guns (not handguns) of sporting value may be auctioned by the city during the regular auction process, unless converted to departmental use. Only those persons possessing an FFL may bid on the weapons.
  - c. Weapons seized pursuant an emergency detention for mental health purposes, must be disposed pursuant the guidelines set forth in Texas Code of Criminal Procedure Art. 18.191. Disposition of firearm seized from certain persons with mental illness.
3. Destruction process for firearms is as follows:
- a. The property custodian ensures the recording of the make, model, serial number, and involved case report number in the property management computer system.

- b. The property custodian destroys firearms authorized for disposal as necessary to conserve space and security of the weapon(s).
  - c. All firearms are inventoried prior to destruction.
  - d. The property custodian updates the new status on all related documents and computer files.
  - e. The property custodian, accompanied by an armed police officer and (if possible) a community volunteer, transports the firearms to a destruction facility. The property custodian, officer, and volunteer witness the destruction of each weapon and sign a certificate certifying the destruction.
  - f. The property custodian retains all written documentation of destruction transactions.
4. Destruction of Ammunition
- a. Department Use
    - i. Surplus small arms and rifle ammunition may be retained by the department for official use.
    - ii. Ammunition retained for department use is transferred to the range master, who signs a receipt for the items and maintains records of the inventory and use of such ammunition.
    - iii. No ammunition of this nature is used for duty purposes.
  - b. Disposal
    - i. The range master has final discretion on the means of ammunition destruction. That officer decides if the ammunition lends itself well to training or other range use.
    - ii. The department employee receiving the ammunition signs the property report. The property report is then forwarded to the property custodian.
5. Destruction of Narcotics/Controlled Substances
- a. The property custodian destroys controlled substances and narcotic paraphernalia after receiving authorization for such disposal.
  - b. If a controlled substance is evidence in a criminal case filed with the county attorney, destruction may not take place until the case is disposed of and authority for disposal is given by the prosecutor assigned to the court. This authorization shall be written and noted on the request-for-disposal form. Other controlled substances may be disposed of summarily by the department.



- c. Items to be destroyed are pulled from their storage locations and placed in boxes labeled “Narcotics Destruction.” Each box is sealed, labeled, and numbered.
  - d. The property custodian prepares a list of applicable case numbers for each box and attaches a copy of the related property reports.
  - e. The property custodian sets an appointment for disposal (crush or burn) and obtains the necessary permits in advance.
  - f. An officer accompanies the property custodian and a person not connected with the department while transporting the controlled substances to the disposal facility. Each attendee witnesses the destruction of the controlled substances and signs a statement to that effect. The contents of the statement comply with the Texas Administrative Code, Title 37, Rule 13.163.
6. Disposal of Hazardous Materials: The disposal of hazardous materials falls under several state and federal statutes. In practice, most disposals are regulated by law. Whenever questions arise regarding the proper procedures for waste disposal, the property custodian consults with the Teague Volunteer Fire Department’s hazardous materials unit for direction and assistance with disposal efforts.

### **XIII. AUCTION OF UNCLAIMED PROPERTY**

#### **A. Disposition of Unclaimed Property**

1. Found property of value not claimed within 90 days is subject to auction. Stolen or embezzled property is subject to auction if unclaimed by the owner after notification of a 90-day limit to reclaim the item.
2. Unclaimed property not governed by statute after being held 90 days from the date the owner was notified to claim the property is subject to auction, destruction, or diversion to department use.

#### **B. Auction of Unclaimed Property**

1. Unclaimed property may be auctioned by the city or may be auctioned by a private company contracted by the city.
2. To avoid conflict of interest, or any appearance of conflict of interest, no employee of the department purchases any item at such auction, either personally or through a third party.

### **XIV. INSPECTIONS (TEXAS BEST PRACTICES: 12.07)**


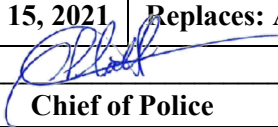
For purposes of this manual, an inspection is defined as a brief, informal, usually unannounced review of procedures, records, or facilities to ensure adherence to policy and established protocol.

- A. The Chief of Police appoints an individual to conduct an inspection of the property room at least every six months and forwards a report of the inspection to the Chief of Police.
- B. The inspection should concentrate on how the policies, procedures, and practices are followed. This inspection should be conducted by a supervisor or another officer not involved in the operation of the property room. The person inspecting the property room should become familiar with property room policies and determine if these policies are being followed. The inspection should include inspection of the security of the property room, the proper use of the sign-in log, the proper and up-to-date processing of property; both intake and disposal, the cleanliness and orderliness of the property room, and any unusual circumstances. The inspection will also require the property custodian to find a minimum of six items randomly selected from the property log by the person inspecting, to include at least one weapon, one drug and one money item.
- C. The Chief of Police may personally conduct frequent unscheduled; unannounced inspections of the property room and property function or assign someone for these inspections, as deemed appropriate. Documentation of these inspections reflects the date and results of that inspection.

**XV. PROPERTY INVENTORIES (TEXAS BEST PRACTICES: 12.08)**

- A. It is the policy of police services to receive and safely store evidence, found property and property for safekeeping; and to restore the property to the rightful owner, or otherwise lawfully dispose of the property in a timely fashion. The division uses the inspection and inventory process to ensure the integrity of this policy.
- B. For purposes of this manual, an inventory is defined as a physical inspection and verification of the location of a property item maintained by the division against the agency's records.
  - 1. A complete inventory is conducted (1) at least once a year, (2) anytime a personnel change is made in the property room, or (3) when requested by the Chief of Police.
    - a. The Chief of Police will assign an officer not connected to the operation of the property room to assist and observe the inventory. The property custodian will conduct the inventory with the assistance of the assigned individual.
    - b. Every item stored in the property system must be accounted for. All property storage areas, rooms, and sites are included in the inventory process.
    - c. All packages, containers, or property tags are inventoried and reconciled with the computer or file system.
    - d. A copy of the inventory report is completed after each inventory and forwarded to the Chief of Police. This report includes any discrepancies and lists any missing items. The Chief of Police decides if an investigation into the loss is warranted.
  - 2. A sampling inventory of individual items stored in the property room at least once a year, anytime a personnel change is made in the property room, or when requested by the Chief of Police.

- a. The Chief of Police will assign an officer not connected to the operation of the property room to assist and observe the inventory. The property custodian will conduct the inventory with the assistance of the assigned individual.
  - b. Sampling will include developing a random sampling process and sampling the number of items required for a 95% assurance with a +/- 3% error. The sampling process will rigidly follow the random sampling process and be documented. If more than a 4% error rate is determined, the Chief of Police shall order a complete inventory of the property room.
  - c. A copy of the inventory report is completed after each inventory and forwarded to the Chief of Police. This report includes any discrepancies and lists any missing items. The Chief of Police determines whether an investigation into the loss is warranted.
- C. Whenever a firearm, money, or controlled substances are discovered missing, the Chief of Police is notified immediately, and an investigation initiated.

	<b>TEAGUE POLICE DEPARTMENT</b>	
	<b>Policy 12.0 Criminal Justice Information Services (CJIS)</b>	
	<b>Effective Date: November 15, 2021</b>	<b>Replaces: All Previous Versions</b>
	<b>Approved:</b> _____  <b>Chief of Police</b>	
	<b>Reference: CJIS Security Policy Version 5.9 (06/01/2020)</b>	

**I. Purpose:**

To establish guidelines for use and security of the department issued TLETS Terminal, Mobile Data Terminal (MDT) equipment and related CJIS information. Failure to comply with this policy can result in disciplinary action or termination.

**II. Policy:**

It shall be the policy of Teague Police Department to protect the integrity of the CJIS database and all data and information obtained through use of Mobile Data Terminals and/or hard-wired TLETS terminals by strictly following the procedures outlined in this General Order.

**III. Definitions:**

- A. TLETS Terminal – This term includes all computers (normally desktop) that have access, via wireless or hardwired network, to TLETS, TCIC, NCIC or any law enforcement database.
- B. MDT -Mobile Data Terminal. This term includes all computers that have access, via wireless or hardwired network, to TLETS, TCIC, NCIC or any law enforcement database.
- C. Secure location -This term includes the areas of Teague Police Department that are not open to the public and accessible only by authorized personnel. This term also includes official police vehicles that are locked and/or attended by authorized sworn police personnel.
- D. Non-secure location -This term includes all locations not defined as "secure location" above.

**IV. Procedures:**

- A. CJIS, TLETS, TCIC and NCIC data shall be accessed ONLY from secure locations, as defined above.

- B. Each person authorized to access Terminal/MDT data shall receive security awareness training within six months of appointment or employment and thereafter at least every two years, in accordance with CJIS policy; this training will be documented.
- C. Maintain a roster and/or agency-issued credentials (officer badge, access card, etc.) of authorized personnel with unescorted access into physically secure areas.
- D. When transporting non-law enforcement personnel in police vehicles, officers will close the screen of the MDT or position it in a manner that will prevent unauthorized viewing of MDT data. TLETS terminal screens shall be positioned to prevent unauthorized viewing.
- E. User/Operator List shall be reviewed annually and as needed; document when this was performed. Changes in authorized personnel (creating, activating, modifying, disabling & removing accounts) will be immediately reported to TCIC Training section.
- F. All printouts of CJIS data shall be promptly filed with the corresponding incident records. Otherwise, such printouts should be promptly shredded; if not shredded, then incinerated. Disposal or destruction is witnessed or carried out by authorized personnel.
- G. All storage media containing or used for CJIS data that is no longer used shall be secure-formatted using methodology that over-writes all data in three iterations or degaussed prior to disposal or release for reuse by unauthorized personnel; if no longer needed, media will be destroyed. Inoperable electronic media shall be physically destroyed. Sanitation or destruction is witnessed or carried out by authorized personnel.
- H. The Department shall keep a list of all MDT IDs and contact(s) so that devices can be promptly disabled, should the need arise.
- I. The local CJIS network equipment shall be in a physically secure location.
- J. All law enforcement vehicles containing MDTs shall be securely locked when not in use.
- K. All computers used for processing CJIS data shall have anti-virus software installed; all will have latest available updates for the operating system & anti-virus. MDT(s) shall have a personal firewall enabled
- L. Employ a Formal Incident Response Plan. It shall be the responsibility of each authorized user to report any violations of this security policy up the chain-of-command and/or proper authorities.
- M. No personal hardware (PC, laptop, etc.) or software shall be allowed on the agency's TLETS network.
- N. No publicly accessible computers shall be allowed on the agency's TLETS network.
- O. The agency shall authorize and control information system-related items entering and exiting the physically secure location.

P. The agency shall establish a Security Alert and Advisories process.

**V. Best Practices:**

A. Periodically check to ensure Servers/Terminals/MDTs connected to the CJIS network are receiving the latest updates regarding the Operating System & Antivirus software; ensure personal firewalls are enabled on MDTs; ensure Sessions are locked within thirty (30) minutes on non-dispatch Terminals. Take appropriate action if required.

B. Periodically check physically secure location(s) to ensure safeguards such as locks are in working order; Doors are closed & properly secured; Terminals are not viewable by unauthorized personnel. Take appropriate action if required.

C. Periodically check to ensure that all network components (routers, firewalls, switches) that process CJIS information are still supported by the manufacturer. If warranties/contracts are in place, ensure they are valid and not out of date. Take appropriate action if required.

D. Periodically check pertinent documents to ensure they are up to date. Take appropriate action such as making editing changes or replacement if required.



## Communicating with People Who Are Deaf or Hard of Hearing

### ADA Guide for Law Enforcement Officers

As a law enforcement officer, you can expect to come into contact with people who are deaf or hard of hearing. It is estimated that up to nine percent of the population has some degree of hearing loss, and this percentage will increase as the population ages.

Under the Americans with Disabilities Act (ADA), people who are deaf or hard of hearing are entitled to the same services law enforcement provides to anyone else. They may not be excluded or segregated from services, be denied services, or otherwise be treated differently than other people. Law enforcement agencies must make efforts to ensure that their personnel communicate effectively with people whose disability affects hearing. This applies to both sworn and civilian personnel.



A driver who is deaf writes on a pad of paper to communicate with an officer.

Your agency has adopted a specific policy regarding communicating with people who are deaf or hard of hearing. It is important to become familiar with this policy.

### Requirements for Effective Communication

The ADA requires that . . .

- Law enforcement agencies must provide the communication aids and services needed to communicate effectively with people who are deaf or hard of hearing, except when a particular aid or service would result in an undue burden or a fundamental change in the nature of the law enforcement services being provided.
- Agencies must give primary consideration to providing the aid or service requested by the person with the hearing disability.
- Agencies cannot charge the person for the communication aids or services provided.
- Agencies do *not* have to provide personally prescribed devices such as hearing aids.
- When interpreters are needed, agencies must provide interpreters who can interpret effectively, accurately, and impartially.
- Only the head of the agency or his or her designee can make the determination that a particular aid or service would cause an undue burden or a fundamental change in the nature of the law enforcement services being provided.

Your agency's policy explains how to obtain interpreters or other communication aids and services when needed.

### Communicating with People Who are Deaf or Hard of Hearing

Officers may find a variety of communication aids and services useful in different situations.

- Speech supplemented by gestures and visual aids can be used in some cases.

- A pad and pencil, a word processor, or a typewriter can be used to exchange written notes.
- A teletypewriter (TTY, also known as a TDD) can be used to exchange written messages over the telephone.
- An assistive listening system or device to amplify sound can be used when speaking with a person who is hard of hearing.
- A sign language interpreter can be used when speaking with a person who knows sign language.
- An oral interpreter can be used when speaking with a person who has been trained to speech read (read lips). **Note:** Do not assume that speech reading will be effective in most situations. On average, only about one third of spoken words can be understood by speech reading.

The type of situation, as well as the individual's abilities, will determine which aid or service is needed to communicate effectively.

### **Practical Suggestions for Communicating Effectively**

- Before speaking, get the person's attention with a wave of the hand or a gentle tap on the shoulder.
- Face the person and do not turn away while speaking.
- Try to converse in a well-lit area.
- Do not cover your mouth or chew gum.
- If a person is wearing a hearing aid, do not assume the individual can hear you.
- Minimize background noise and other distractions whenever possible.
- When you are communicating orally, speak slowly and distinctly. Use gestures and facial expressions to reinforce what you are saying.
- Use visual aids when possible, such as pointing to printed information on a citation or other document.
- Remember that only about one third of spoken words can be understood by speech reading.
- When communicating by writing notes, keep in mind that some individuals who use sign language may lack good English reading and writing skills.
- If someone with a hearing disability cannot understand you, write a note to ask him or her what communication aid or service is needed.
- If a sign language interpreter is requested, be sure to ask *which* language the person uses. American Sign Language (ASL) and Signed English are the most common.
- When you are interviewing a witness or a suspect or engaging in any complex conversation with a person whose primary language is sign language, a qualified interpreter is usually needed to ensure effective communication.
- When using an interpreter, look at and speak directly to the deaf person, not to the interpreter.
- Talk at your normal rate, or slightly slower if you normally speak very fast.
- Only one person should speak at a time.
- Use short sentences and simple words.



- Do not use family members or children as interpreters. They may lack the vocabulary or the impartiality needed to interpret effectively.

## **What Situations *Require* an Interpreter?**

Generally, interpreter services are not required for simple transactions – such as checking a license or giving directions to a location – or for urgent situations – such as responding to a violent crime in progress.

**Example:** An officer clocks a car on the highway going 15 miles per hour above the speed limit. The driver, who is deaf, is pulled over and is issued a noncriminal citation. The individual is able to understand the reason for the citation because the officer points out relevant information printed on the citation or written by the officer.

**Example:** An officer responds to an aggravated battery call and upon arriving at the scene observes a bleeding victim and an individual holding a weapon. Eyewitnesses observed the individual strike the victim. The individual with the weapon is deaf. Because the officer has probable cause to make a felony arrest without an interrogation, an interpreter is not necessary to carry out the arrest.

However, an interpreter may be needed in lengthy or complex transactions – such as interviewing a victim, witness, suspect, or arrestee – if the person being interviewed normally relies on sign language or speech reading to understand what others are saying.

**Example:** An officer responds to the scene of a domestic disturbance. The husband says the wife has been beating their children and he has been trying to restrain her. The wife is deaf. The officer begins questioning her by writing notes, but her response indicates a lack of comprehension. She requests a sign language interpreter. In this situation an interpreter should be called. If the woman's behavior is threatening, the officer can make an arrest and call for an interpreter to be available later at the booking station.

It is inappropriate to ask a family member or companion to interpret in a situation like this because emotional ties may interfere with the ability to interpret impartially.

**Example:** An officer responds to the scene of a car accident where a man has been seriously injured. The man is conscious, but is unable to comprehend the officer's questions because he is deaf. A family member who is present begins interpreting what the officer is saying.

A family member or companion *may* be used to interpret in a case like this, where the parties are willing, the need for information is urgent, and the questions are basic and uncomplicated. However, in general, do not expect or demand that a deaf person provide his or her own interpreter. As a rule, when interpreter service is needed, it must be provided by the agency.

List your agency's contact information for obtaining an interpreter, an assistive listening device, or other communication aid or service here.

**For further information on the Americans with Disabilities Act contact:**

**ADA Website**

[www.ada.gov](http://www.ada.gov)

**ADA Information Line**

800-514-0301 (voice)

800-514-0383 (TTY)

This pamphlet was developed by the U.S. Department of Justice for law enforcement personnel.

**Reproduction is encouraged.**

January 2006

---

p

# Employee Leave Request

Name: \_\_\_\_\_

Date: \_\_\_\_\_

Department: \_\_\_\_\_

Requested Date(s) Off: \_\_\_\_\_

Time Requested: \_\_\_\_\_ Hours Requested: \_\_\_\_\_

Vacation \_\_\_\_\_ Comp. Time \_\_\_\_\_ Sick Leave \_\_\_\_\_ Other \_\_\_\_\_

Explanation: \_\_\_\_\_

*Physician Documentation may be required at the request of the Supervisor or City Administrator.*

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

---

## Supervisor's Use Only

Time Off: Approved  Denied

\_\_\_\_\_  
Supervisor Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
City Admin/Secretary Signature

\_\_\_\_\_  
Date

## Teague Police Department Equipment Issue/Return Form

Employee Name: \_\_\_\_\_

ID#: \_\_\_\_\_

<i>Item and Serial Number (if required)</i>	<i>Auth</i>	<i>Number Issued</i>	<i>Number Returned</i>	<i>Notes/ Condition</i>
Uniform Trousers	3			
Short-sleeved uniform shirts	3			
Long-sleeved uniform shirts	3			
Tie	1			
Garrison cap	1			
Cap badge	1			
Shirt badge	1			
Name plate	1			
Raincoat	1			
Cap rain cover	1			
Winter jacket	1			
Trouser Belt	1			
Sam Browne Belt	1			
Holster	1			
Handcuff Case	1			
Magazine Case	1			
Radio Case	1			
Bio-glove case	1			
Baton Holder	1			
Protective vest (body armor)	1			
Traffic vest	1			
Baton (ASP)	1			
Handcuffs	1			
Duty Handgun Serial Number:	1			
Handgun Magazines (3)	3			
Taser Serial Number:	1			
Taser Cartridges, Serial numbers:	2			
OC Spray	1			
OC Spray carrier	1			
Traffic Ticket Holder	1			
Policy Manual with Updates	1			

Employee Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Equipment Officer Signature: \_\_\_\_\_

**FREESTONE COUNTY MAGISTRATE'S INFORMATION  
FAMILY VIOLENCE / STALKING / VIOLATION OF PROTECTIVE ORDER OFFENSE**

**Defendant's Information**

RELATIONSHIP TO VICTIM:  SPOUSE  EX-SPOUSE  ROOMMATE  HAD A CHILD TOGETHER  OTHER: \_\_\_\_\_  
DEFENDANT'S NAME: \_\_\_\_\_ SEX:  M  F DOB: \_\_\_\_\_  
HOME ADDRESS: \_\_\_\_\_ OWNER/PRIMARY LESSEE: YES OR NO  
NAME OF DEFENDANT'S EMPLOYER: \_\_\_\_\_  
PRIOR FV / STALKING / VIOL OF PROTECTIVE ORDER ARRESTS: \_\_\_\_\_  
PRIOR CONVICTIONS FOR ABOVE: \_\_\_\_\_  
CONVICTION DATES: \_\_\_\_\_  
ON PROBATION?  YES  NO PROBATION OFFICER'S NAME: \_\_\_\_\_  
KNOWN SERIOUS MENTAL PROBLEMS: \_\_\_\_\_ WEAPONS OWNED: \_\_\_\_\_  
AT TIME OF OFFENSE, HAD DEFENDANT BEEN USING DRUGS OR ALCOHOL?  YES  NO  UNKNOWN

**HISTORY OF FAMILY VIOLENCE**

YES  NO FIRST TIME OCCURRENCE? IF NOT, DOCCUMENT ALL REPORTED AND UNREPORTED INCIDENTS:  
\_\_\_\_\_  
 YES  NO PRIOR 911 CALLS FROM VICTIM'S ADDRESS REGARDING THIS FAMILY?  
 YES  NO IS FAMILY VIOLENCE LIKELY TO OCCUR IN THE FORESEEABLE FUTURE?

**DOMESTIC VIOLENCE RISK ASSESSMENT**

CHECK APPROPRIATE ITEMS

<input type="checkbox"/> GUN PRESENT IN HOME OR ACCESSIBLE TO SUSPECT	<input type="checkbox"/> SUSPECT ABUSES ALCOHOL
<input type="checkbox"/> SUSPECT HAS USED OR THREATENED TO USE A WEAPON	<input type="checkbox"/> SUSPECT USES ILLEGAL/ABUSES LEGAL DRUGS
<input type="checkbox"/> PARTIES RECENTLY SEPARATED/THREATENED SEPARATION	<input type="checkbox"/> SUSPECT VIOLENT OUTSIDE OF RELATIONSHIP
<input type="checkbox"/> INCREASE IN FREQUENCY OR SEVERITY OF VIOLENCE	<input type="checkbox"/> SUSPECT HAS ACCUSED VICTIM OF CHEATING
<input type="checkbox"/> SUSPECT HAS DESTROYED CHERISHED PERSONAL ITEMS	<input type="checkbox"/> SUSPECT THREATENS TO KILL
<input type="checkbox"/> SUSPECT HAS SAID, "IF I CAN'T HAVE YOU, NO ONE CAN"	<input type="checkbox"/> SUSPECT VIOLENT TOWARD CHILDREN
<input type="checkbox"/> SUSPECT CONTEMPLATED/THREATENED/ATTEMPTED SUICIDE	<input type="checkbox"/> SUSPECT HAS INJURED OR KILLED PETS
<input type="checkbox"/> VICTIM CONTEMPLATED/THREATENED/ATTEMPTED SUICIDE	<input type="checkbox"/> VICTIM IS CURRENTLY PREGNANT
<input type="checkbox"/> SUSPECT DIRECTED VIOLENCE TOWARD PREGNANT PARTNER	<input type="checkbox"/> SUSPECT HAS FORCED VICTIM TO HAVE SEX
<input type="checkbox"/> SUSPECT IS JEALOUS OR ATTEMPTS TO CONTROL PARTNERS DAILY ACTIVITIES	
<input type="checkbox"/> ADDITIONAL INFORMATION _____	

**EMERGENCY PROTECTIVE ORDER – 24 HOUR FV HOLD**

REQUESTED BY:  VICTIM  GUARDIAN OF VICTIM  PEACE OFFICER  STATE'S ATTORNEY  NONE

YES  NO INVESTIGATING OFFICER BELIEVES VICTIM MAY NEED PRETECTIVE ORDER BUT IS AFRAID OF DEFENDANT AND IS RELUCTANT TO ASK

YES  NO INVESTIGATING OFFICER BELIEVES A PROTECTIVE ORDER WOULD BE APPROPRIATELY ISSUED ON THE MAGISTRATE'S OWN MOTION

YES  NO INVESTIGATING OFFICER BELIEVES A 24 HOUR FV HOLD SHOULD BE ISSUED BY THE MAGISTRATE?  
IF YES, WHY? \_\_\_\_\_

**VICTIM'S ("PROTECTED PERSON") INFORMATION**

VICTIM'S NAME: \_\_\_\_\_ SEX:  M  F DOB: \_\_\_\_\_  
RACE:  INDIAN  ASIAN  BLACK  WHITE  UNKNOWN ETHNICITY:  HISPANIC  NON-HISPANIC  UNKNOWN  
HOME ADDRESS: \_\_\_\_\_ CITY & ZIP \_\_\_\_\_  
HOME PHONE: \_\_\_\_\_ OWNER/PRIMARY LESSEE:  YES  NO  
OTHER OCCUPANTS IN HOME: \_\_\_\_\_  
NAME OF VICTIM'S EMPLOYER: \_\_\_\_\_  
EMPLOYER ADDRESS: \_\_\_\_\_ CITY & ZIP \_\_\_\_\_  
WORK PHONE: \_\_\_\_\_ WORK HOURS: \_\_\_\_\_ OTHER PHONE #s: \_\_\_\_\_  
VICTIM RELOCATING TO OTHER ADDRESS: \_\_\_\_\_  
 PERMANENT RELOCATION  TEMPORARY RELOCATION FOR \_\_\_\_\_ # of DAYS PHONE: \_\_\_\_\_  
 VICTIM REQUESTS THIS ADDRESS BE OMITTED FROM THE ORDER FOR THE VICTIM'S SAFETY  
AT TIME OF OFFENSE, HAD VICTIM BEEN USING DRUGS OR ALCOHOL?  YES  NO  UNKNOWN

**PROTECTED CHILD INFORMATION**

WHO IS PRIMARY CARETAKER OF THE CHILD/CHILDREN? \_\_\_\_\_  
1) NAME: \_\_\_\_\_ DOB: \_\_\_\_\_ SEX:  M  F  
NAME OF SCHOOL/DAY CARE: \_\_\_\_\_  
SCHOOL/DAY CARE ADDRESS: \_\_\_\_\_ CITY & ZIP \_\_\_\_\_  
2) NAME: \_\_\_\_\_ DOB: \_\_\_\_\_ SEX:  M  F  
NAME OF SCHOOL/DAY CARE: \_\_\_\_\_  
SCHOOL/DAY CARE ADDRESS: \_\_\_\_\_ CITY & ZIP \_\_\_\_\_  
3) NAME: \_\_\_\_\_ DOB: \_\_\_\_\_ SEX:  M  F  
NAME OF SCHOOL/DAY CARE: \_\_\_\_\_  
SCHOOL/DAY CARE ADDRESS: \_\_\_\_\_ CITY & ZIP \_\_\_\_\_  
4) NAME: \_\_\_\_\_ DOB: \_\_\_\_\_ SEX:  M  F  
NAME OF SCHOOL/DAY CARE: \_\_\_\_\_  
SCHOOL/DAY CARE ADDRESS: \_\_\_\_\_ CITY & ZIP \_\_\_\_\_

**THE FOLLOWING ITEMS ARE ATTACHED IF AVAILABLE:**

VICTIM AND/OR WITNESS STATEMENTS  
 INFORMATION ON 911 CALLS  
 ADDITIONAL COMMENTS: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

ON THOSE CASES FILES WHERE A WARRANT IS ISSUED,  
**THE INVESTIGATING OFFICER SHALL COMPLETE THIS FORM**  
AND ATTACH IT WITH THE OTHER INFORMATION TO THE WARRANT.

# TEAGUE POLICE DEPARTMENT

## Field Identification Form

Case Number: \_\_\_\_\_

**Read the following to the witness:**

1. You will be advised of the procedures for viewing the field identification.
2. The fact that an individual is being shown to you, should not cause you to believe or guess that the guilty person(s) has been identified or arrested.
3. This *may or may not* be the person who committed the crime.
4. You are in no way obligated to identify anyone. It is as important to clear the innocent as it is to identify the guilty.
5. Regardless of whether you make an identification, the police will continue to investigate this incident.
6. If you recognize anyone, please tell me how you recognize the individual. We are required to ask you to state in your own words, how certain you are of any identification.

I, \_\_\_\_\_ understand the above information.

I understand the need to describe my level of certainty regarding identification and after viewing the person(s) shown have identified them as \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Viewer's Signature: \_\_\_\_\_

Officer's printed name: \_\_\_\_\_

Officer's signature: \_\_\_\_\_

Other persons in attendance during field identification.

Name and Address: \_\_\_\_\_

Name and Address: \_\_\_\_\_

**TEAGUE POLICE DEPARTMENT  
INFORMANT AGREEMENT**

During my association with the TEAGUE Police Department as an Informant, I, the undersigned, do hereby agree to be bound by the following conditions and procedures while so associated:

1. I agree that I have no police power under the State of Texas or any local governmental subdivision and have no authority to carry a weapon while performing my activity as an Informant.
2. I acknowledge that I am associated with the Teague Police Department as an Informant on a case or time basis as an independent contractor and that any payment I receive from the TEAGUE Police Department will not be subject to Federal or State Income Tax Withholding or Social Security. All reporting of income is the responsibility of the Informant.
3. I further acknowledge that as an Informant and independent contractor, I am not entitled to Workman's Compensation or Unemployment Compensation from the State of Texas and I shall not hold Freestone County liable for any injuries or damage incurred by reason of my association with the Teague Police Department.
4. I further agree not to divulge to any person, except the investigator with whom I am associated, my status as an Informant for the Teague Police Department unless required to do so in court and shall not represent myself to others as an employee or representative of the Teague Police Department.
5. I further agree not to use the Teague Police Department or any of its officers as credit references or employment references unless prior approval is obtained from the investigator with whom I am associated.
6. I further agree that my association with the Teague Police Department does not afford me any special privileges. I understand that I can have no personal or social relationship with any officer or member of the Teague Police Department.
7. I further agree that after making a purchase of anything of evidentiary value, I will contact the investigator with whom I associated as soon as possible for delivery of such evidence to him.
8. I further agree to maintain a strict accounting of all funds provided to me by the Teague Police Department as part of my activity as an Informant. I understand that misuse of funds could be grounds for criminal prosecution against me.
9. Finally, I agree that violation of any of the above enumerated provisions will be grounds for immediate termination and probable criminal charges.

Dated this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_\_.

Informant \_\_\_\_\_

Investigator \_\_\_\_\_



Notification--Emergency Detention NO. \_\_\_\_\_

DATE: \_\_\_\_\_ TIME: \_\_\_\_\_

THE STATE OF TEXAS  
FOR THE BEST INTEREST AND PROTECTION OF:

\_\_\_\_\_

NOTIFICATION OF EMERGENCY DETENTION

Now comes \_\_\_\_\_, a peace officer with (name of agency) Teague Police Department, Freestone County, of the State of Texas, and states as follows:

1. I have reason to believe and do believe that (name of person to be detained) \_\_\_\_\_ evidences mental illness.

2. I have reason to believe and do believe that the above-named person evidences a substantial risk of serious harm to himself/herself or others based upon the following:

\_\_\_\_\_

3. I have reason to believe and do believe that the above risk of harm is imminent unless the above-named person is immediately restrained.

4. My beliefs are based upon the following recent behavior, overt acts, attempts, statements, or threats observed by me or reliably reported to me:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

5. The names, addresses, and relationship to the above-named person of those persons who reported or observed recent behavior, acts, attempts, statements, or threats of the above-named person are (if applicable):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

For the above reasons, I present this notification to seek temporary admission to the (name of facility) \_\_\_\_\_ inpatient mental health facility or hospital facility for the detention of (name of person to be detained) \_\_\_\_\_ on an emergency basis.

6. Was the person restrained in any way? Yes  No

\_\_\_\_\_  
PEACE OFFICER'S SIGNATURE

BADGE NO. \_\_\_\_\_

Address: 315 Main Street Teague, Texas Zip Code: 75860

Telephone: (254) 739-2553



# Teague Police Department

315 Main Street

Teague, Texas 75860

Phone: (254) 739-2553 Fax: (254) 739-3213

DeWayne Philpott, Chief of Police

## TEAGUE POLICE DEPARTMENT NOTIFICATION OF STUDENT ARREST OR REFERRAL

Name: \_\_\_\_\_ Address: \_\_\_\_\_

Race: Sex: DOB: Campus: Grade:

This written notice, required by article 15.27 Texas Code of Criminal Procedure, is to inform you that the above listed student has been arrested or referred for any felony offense AND/OR the following Misdemeanor offense(s):

(1) Felony Offense(s):

(2) Misdemeanor Offense(s):

- |   |  |
|---|--|
| <input type="checkbox"/> 20.02 – Unlawful Restraint   | <input type="checkbox"/> 21.08 – Indecent Exposure               |
| <input type="checkbox"/> 22.01 – Assault  | <input type="checkbox"/> 22.05 – Deadly Conduct                  |
| <input type="checkbox"/> 22.07 – Terroristic Threat   | <input type="checkbox"/> Engaging in Organized Criminal Activity |
| <input type="checkbox"/> 28.03 – Criminal Mischief  |  |
| <input type="checkbox"/> Unlawful use, sale or possession of a controlled substance, drug paraphernalia or marijuana. |  |
| <input type="checkbox"/> Unlawful possession of any weapons or devices listed in sections 46.01 (1-14 or 16).         |  |
| <input type="checkbox"/> Prohibited weapon under section 46.05.   |  |

Date of Arrest: \_\_\_\_\_ Teague Police Department Case Number: \_\_\_\_\_

Case Synopsis:

### WARNING

The information contained in this notice is intended only to inform appropriate school personnel of an arrest or referral of a student believed to be enrolled in this school. An arrest or referral should not be construed as proof that a student is guilty. Guilt is determined in a court of law.

**THE INFORMATION CONTAINED IN THIS NOTICE IS PERSONAL AND CONFIDENTIAL!**

If you have any questions concerning this notice, please contact:  
Chief DeWayne Philpott – [policechief@cityofteaguetx.com](mailto:policechief@cityofteaguetx.com)  
254-739-2553

*Honesty, Integrity, Pride*

**OUTSIDE EMPLOYMENT AUTHORIZATION FORM**

**City of Teague**

I \_\_\_\_\_ seek authorization from the City to pursue outside employment, in this area:

For Outside Employer: \_\_\_\_\_ Address: \_\_\_\_\_

Outside Employer Supervisor: \_\_\_\_\_ Bus. Phone: \_\_\_\_\_

New request \_\_\_\_\_ Annual Request \_\_\_\_\_ Hours to be worked \_\_\_\_\_

If new, starting date \_\_\_\_\_ Hours per week \_\_\_\_\_

During this outside employment, I will engage in these activities (**both specific and general**):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

I acknowledge that if I am injured in the course of any outside employment, it is not proper to seek workers compensation benefits from the City. I hereby waive all rights of workers compensation against the City's carrier that are in any way related to the tasks, activities, etc., to the performance and/or pursuit of my outside employment. I further understand and acknowledge that I must advise the outside employer of this policy and his/her potential worker's compensation responsibility if I receive an injury or illness. INITIAL HERE: \_\_\_\_\_

I further understand and acknowledge that I must provide the City with a copy of the outside employer's worker's compensation coverage on an annual or as-requested basis. INITIAL HERE \_\_\_\_\_

I acknowledge that this Authorization Form does not indicate that the City approves or in any manner endorses my outside employment. I hereby release the City from any liability that may arise against me while engaged in this outside employment. INITIAL HERE \_\_\_\_\_

I acknowledge that it is a violation of City policies to engage in outside employment activities when I do not report for the City job due to injury, sick leave, FMLA leave, whether paid or unpaid, disability leave, or an unpaid leave of absence. I acknowledge that I am not to use any City equipment, uniforms, supplies, tools etc, in connection with my outside employment. I also agree to not conduct any business related to my outside employment during my regular duty hours. INITIAL HERE \_\_\_\_\_

I acknowledge that if my outside employment begins to interfere with the effective performance of assigned City duties, I shall be required to terminate the outside employment or resign from the City's employment. INITIAL HERE \_\_\_\_\_

\_\_\_\_\_  
SUBMITTING EMPLOYEE \_\_\_\_\_ DATE \_\_\_\_\_

SUPERVISOR \_\_\_\_\_  APPROVED  DENIED  
DATE \_\_\_\_\_

CHIEF OF POLICE \_\_\_\_\_  APPROVED  DENIED  
DATE \_\_\_\_\_

CITY ADMINISTRATOR \_\_\_\_\_  APPROVED  DENIED  
DATE \_\_\_\_\_

DATE ELIGIBLE TO START \_\_\_\_\_

**SWORN POLICE OFFICER**  
**PERFORMANCE EVALUATION**

NAME \_\_\_\_\_

**PERFORMANCE RATING INSTRUCTIONS:**

RANK/ASSIGNMENT \_\_\_\_\_

The narrative portion of the evaluation follows the scale ratings. Refer to the rating guide for an explanation of the rated behaviors. Raters may comment on any observed behavior, but specific comments are required to justify ratings of "1," "2," or "5."

EVALUATION PERIOD \_\_\_\_\_

DATE OF EVALUATION \_\_\_\_\_

<b>Unacceptable</b>	<b>Acceptable</b>	<b>Superior</b>	<b>Not Observed</b>
<b>1</b>	<b>2 3</b>	<b>4 5</b>	

**PART I: PERFORMANCE TASKS**

(1)	Driving skills (stress conditions)	1	2	3	4	5	N.O. ____
(2)	Driving Skills (non-stress conditions)	1	2	3	4	5	N.O. ____
(3)	Orientation skills	1	2	3	4	5	N.O. ____
(4)	Field performance (stress conditions)	1	2	3	4	5	N.O. ____
(5)	Field performance (non-stress cond.)	1	2	3	4	5	N.O. ____
(6)	Officer safety (general)	1	2	3	4	5	N.O. ____
(7)	Officer safety (with suspicious persons and prisoners)	1	2	3	4	5	N.O. ____
(8)	Control of conflict (voice command)	1	2	3	4	5	N.O. ____
(9)	Control of conflict (physical skill)	1	2	3	4	5	N.O. ____
(10)	Investigative procedures	1	2	3	4	5	N.O. ____
(11)	Report writing (organization/details)	1	2	3	4	5	N.O. ____
(12)	Proper form selection (accuracy and details)	1	2	3	4	5	N.O. ____

	Unacceptable 1	2	Acceptable 3	4	Superior 5		Not Observed	
(13) Report writing (grammar/spelling/neatness)			1	2	3	4	5	N.O. ____
(14) Report writing (appropriate time used)			1	2	3	4	5	N.O. ____
(15) Radio (listens and comprehends transmissions)			1	2	3	4	5	N.O. ____
(16) Radio (articulation of transmissions)			1	2	3	4	5	N.O. ____
<b><u>COMMUNITY POLICING SKILLS</u></b>								
(17) Self-initiated activity			1	2	3	4	5	N.O. ____
(18) Problem-solving/decision-making			1	2	3	4	5	N.O. ____
(19) Community-policing objectives			1	2	3	4	5	N.O. ____
<b><u>KNOWLEDGE</u></b>								
(20) Knowledge of department orders			1	2	3	4	5	N.O. ____
(21) Knowledge of criminal law			1	2	3	4	5	N.O. ____
(22) Knowledge of traffic law			1	2	3	4	5	N.O. ____
<b><u>ATTITUDE/RELATIONS</u></b>								
(23) Acceptance of feedback			1	2	3	4	5	N.O. ____
(24) Relationship with citizens			1	2	3	4	5	N.O. ____
(25) Relationship with co-workers/super.			1	2	3	4	5	N.O. ____
(26) General demeanor			1	2	3	4	5	N.O. ____

Unacceptable                      Acceptable                      Superior                      Not Observed  
1                      2                      3                      4                      5

**APPEARANCE**

(27) General appearance                      1                      2                      3                      4                      5                      N.O. \_\_\_\_

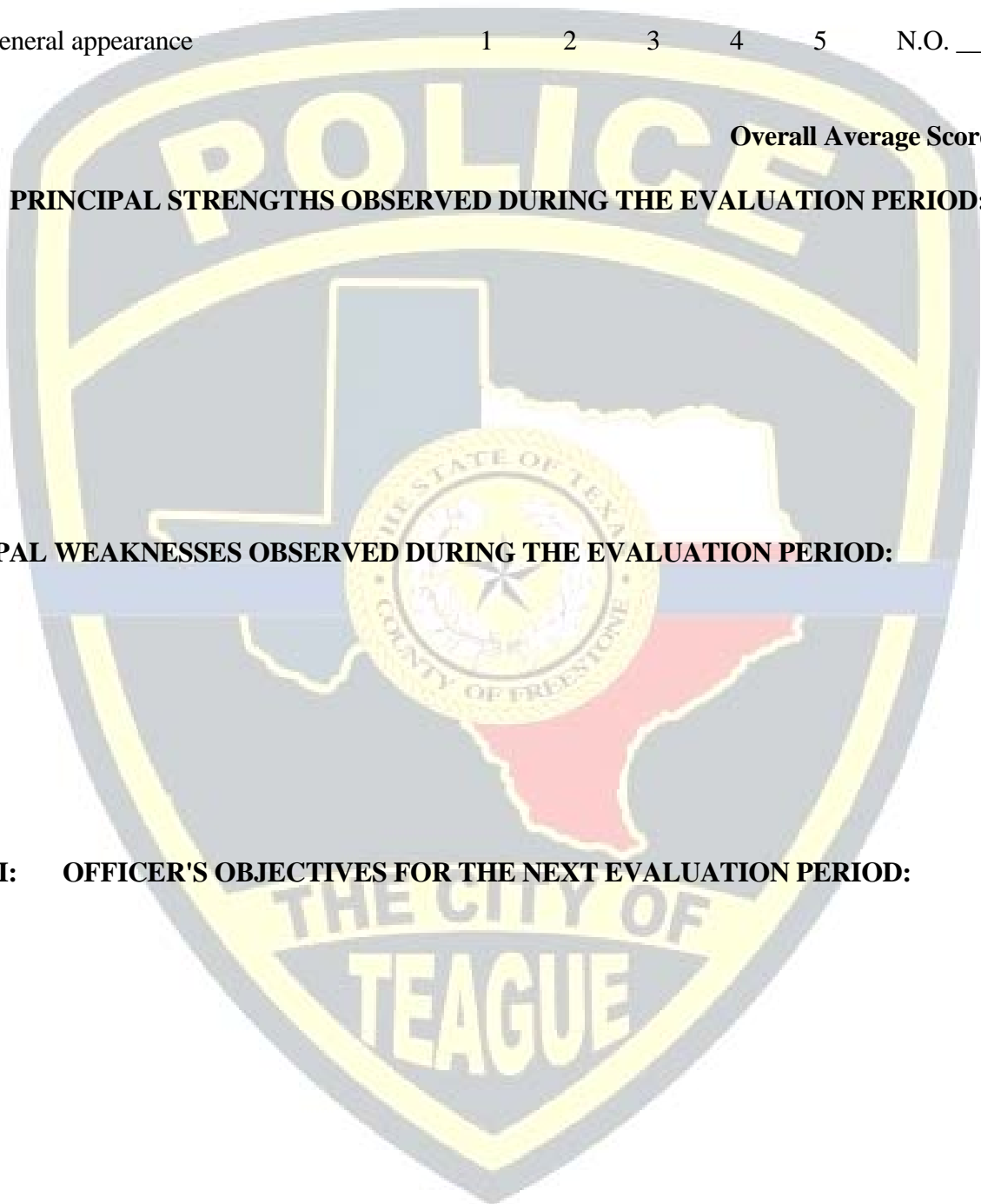
Overall Average Score \_\_\_\_

**Part II: PRINCIPAL STRENGTHS OBSERVED DURING THE EVALUATION PERIOD:**

**PRINCIPAL WEAKNESSES OBSERVED DURING THE EVALUATION PERIOD:**

**PART III: OFFICER'S OBJECTIVES FOR THE NEXT EVALUATION PERIOD:**

- 1.
- 2.
- 3.



**SUPERVISOR'S EVALUATION OF OFFICER'S PROGRESS TOWARDS OBJECTIVES:**



**Rating Authority** \_\_\_\_\_ **Date** \_\_\_\_\_  
(Print name and sign)

**Officer's Signature** \_\_\_\_\_ **Date** \_\_\_\_\_

**Chief's Signature** \_\_\_\_\_ **Date** \_\_\_\_\_

Form Rev.

**TEAGUE POLICE DEPARTMENT  
OVERTIME NOTIFICATION**

Employee Name: \_\_\_\_\_ Employee Number: \_\_\_\_\_

Date earned: \_\_\_\_\_ Hour(s) worked: \_\_\_\_\_

Reason (include case number(s): \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Supervisor who pre-approved hours to be compensated: \_\_\_\_\_

Employee Signature \_\_\_\_\_ Date \_\_\_\_\_

**To be completed and turned in with time card for any time worked over the normal assigned scheduled hours.**



**PERFORMANCE IMPROVEMENT PLAN**

**30 DAY EVALUATION**

Name of Employee: \_\_\_\_\_ Title: \_\_\_\_\_ Date: \_\_\_\_\_

Plan Supervisor: \_\_\_\_\_ Department: \_\_\_\_\_

EVALUATORS: \_\_\_\_\_

AREAS OF IMPROVEMENT: \_\_\_\_\_

AREAS NEEDING IMPROVEMENT: \_\_\_\_\_

RECOMMENDATION: \_\_\_\_\_

ACTION TAKEN: \_\_\_\_\_

Signature of Department Head: \_\_\_\_\_

Evaluator: \_\_\_\_\_ Evaluator: \_\_\_\_\_

Signature of Employee acknowledging receipt of 30 day evaluation for Performance Improvement: \_\_\_\_\_

A lack of performance improvement can lead to further disciplinary actions up to and including termination of employment. A copy of this Evaluation of Performance Improvement will be placed in the Employee's personnel file.

# **IMPORTANT INFORMATION**

## **TCOLE Personal History Statement Template Instructions**

The attached Personal History Statement (PHS) is intended as a sample of what TCOLE considers to be the minimum information necessary to meet the required background investigation (BI) for any law enforcement licensee appointed to an agency, as defined under TCOLE Rule 211.1(a)(8).

Agency administrators may add additional information or agency identifiers without deletion or elimination of any information in this document. They may also decide at which stage in the pre-appointment process the PHS/BI will be completed as long as it is done before the applicant is appointed. The objective is to help the agency's chief administrator to make an informed decision based on factual and verifiable information.

The PHS/BI is an auditable document which must be retained along with all other required TCOLE appointment documents through the licensee's employment and five (5) years after he or she leaves the agency. For training academies, the record must be retained for five (5) years from the last date at the academy.

**TEXAS COMMISSION ON LAW ENFORCEMENT**

**TCOLE**

**AGENCY NAME:**

APPLICANT'S PERSONAL HISTORY STATEMENT

PERSONAL HISTORY STATEMENT FOR TEXAS

Appointment/Employment

Name:

Date Issued:

Complete and Return By:

I am applying for:

Peace Officer                      PID #:

County Jailer                        PID #:

Telecommunicator                PID #:

Civilian Employment

## **Personal History Statement Instructions**

Employees are exposed to confidential and law enforcement sensitive information. A thorough background investigation is required to properly evaluate the suitability of applicants for employment with the agency. Although it is an achievement to reach the background phase of the hiring process, this is still a competitive process and does not, in any way, guaranty selection.

These instructions are provided as a guide to assist you in properly completing your Personal History Statement. It is essential that the information is accurate in all respects, so please read all instructions carefully before proceeding. The Personal History Statement will be used as a basis for a background investigation that will determine your eligibility for becoming an employee.

1. Your application must be printed legibly in **BLACK INK** by the applicant or typed. Answer all questions truthfully and accurately.
2. If a question is not applicable to you, enter **N/A** in the space provided.
3. Avoid errors by reading the directions carefully before making any entries on the form. Be sure your information is accurate and in proper sequence before you begin.
4. You are responsible for obtaining correct and full addresses. If you are not sure of an address, personally verify before making that entry on this history statement. Errors will not be viewed favorably. **ALL ADDRESSES MUST BE COMPLETE WITH ZIP CODES.**
5. If you need additional space for your answers, attach additional sheets as needed. Be sure to indicate what question number and page this refers to.
6. An accurate and complete form will help expedite your investigation. Omissions or falsifications will result in disqualification.
7. You are responsible for furnishing any changes and/or updating your application as needed, such as address changes or telephone changes in writing.
8. Any candidate submitting an incomplete application **WILL NOT BE CONSIDERED FOR EMPLOYMENT.** Your application will be evaluated on completeness and neatness.
9. **All documents requested must be submitted with the application** (photocopies are acceptable in most cases). *Required documents vary according to the position being sought and the history of the applicant. Hiring agency please check off documents required– modify list as necessary.*

Completed Personal History Statement

Copy of your Social Security card

Original certified copy of your birth certificate (no photo copy)

Copy of your valid Texas driver license or a copy of another State's driver license (applicant must possess a valid Texas driver license prior to being offered employment)

Copy of your High School diploma or GED certificate or an honorable discharge from the armed forces of the United States after at least twenty-four months of active service

Sealed original certified copy of your college transcript (no photo copy)

Photocopy of your college diploma

Copy of your Peace Officer Certificate from your police academy (Peace Officer Applicants Only)

Copy of your Texas peace officer license & all training certificates awarded to you (Peace Officer Applicants Only)

Copy of your DD-214 and/or other military discharge documents (if applicable)

Original certified copy of your Naturalization papers, if applicable (no photo copy)

Copy of current proof of automobile liability insurance

Copy of a TCOLE approved Firearms Qualifications within the last 12 months

10. If you have questions, please contact your assigned background investigator.
11. When submitting the completed documents, please place them in a sealed envelope marked 'Personal and Confidential' to your assigned background investigator.

## Instructions to the Applicant

Before you begin to fill out this personal history statement, please ensure that you meet the following requirements. You must meet all five of these requirements to qualify for licensure as a peace officer, jailer, or telecommunicator in Texas.

I am a citizen of the United States of America.

I have earned a high school diploma, a GED, or an honorable discharge from the armed services of the United States after at least two (2) years of active service.

I have never been convicted, plead guilty (nolo contendere), nor have I been on court-ordered community service/probation, or deferred adjudication for a Class A misdemeanor or a felony.

During the last ten (10) years, I have not been convicted, plead guilty (nolo contendere), been on community service/probation, or deferred adjudication for a Class B misdemeanor in this state, other state, or while serving in the military.

I have never had a military court martial that resulted in a dishonorable or other discharge based on misconduct which bars future military service.

### DISQUALIFICATIONS

There are very few automatic bases for rejection. Even issues of prior misconduct, employee terminations, and arrests are usually not, in and of themselves, automatically disqualifying. However, deliberate misstatements or omissions can and often will result in your application being rejected, regardless of the nature or reason for the misstatements/omissions. In fact, the number one reason individuals “fail” background investigations is because they deliberately withhold or misrepresent job-relevant information from their prospective employer.

This personal history statement is a governmental document. Be truthful, as there are criminal consequences for lying on a governmental document.

Once you begin:

- Type or neatly print, in ink, responses to all items and questions. If a question does not apply to you, write “N/A” (not applicable) in the space provided for your response. If you cannot obtain or remember certain information, indicate so in your response.
- If you need additional space for your answers, attach additional sheets as needed. Be sure to indicate which section, question number, and page this refers to.
- Be as complete, honest, and specific as possible in your responses.

### Disclosure of Medically Related Information

In accordance with the U.S. Americans with Disabilities Act, at this stage of the hiring process, applicants are not expected or required to reveal any medical or other disability-related information about themselves in response to questions on this form, or to any other inquiry made prior to receiving a conditional offer of employment.

**SECTION 1: PERSONAL**

Last Name: First Name: Middle Name: Suffix:

Other Names, including nicknames, you have used or been known by:

Maiden: SSN #: Date of Birth:

Driver License #: State: Exp:

Street Address, (Apt/Unit):

City: State: Zip Code:

Mailing Address (if different than above):

City: State: Zip Code:

Home Phone #: Cell: Work (Ext.):

Fax: Other Phone #(s):

List ALL Email Addresses:

Place of Birth (City, County, State, Country):

Physical Description:

Height: Weight: Hair Color: Eye Color:

---

Have you ever attended a basic licensing course? Yes No

If yes, provide the PID you were assigned:

**A.** Academy Name: From: To:

Location (City, State):

Name Training Coordinator: Contact Number:

Did you graduate? Yes No

**B.** Academy Name: From: To:

Location (City, State):

Name Training Coordinator: Contact Number:

Did you graduate? Yes No

Have you **ever** applied to any other law enforcement agency in the last ten years (city, county, state or federal)?

Yes            No

- If yes, list ALL agencies you have applied to, starting with the most recent (give complete and accurate addresses).
- All agencies MUST be listed regardless of the outcome or current status. Check all boxes that apply for each agency.
- If you need additional space for your answers, attach additional sheets as needed. Be sure to indicate what section number and page this refers to.

**A. Name of Agency:**

Position Applied For:

Date Applied:

Address:

City:

State:

Zip:

Background Investigator's Name (if known):

Contact Number, (ext):

Email:

Check each step in the process that you completed, and your status:

<b>Steps:</b>	Application	Written	Physical agility	Oral	Polygraph/CVSA	Background
	Conditional job offer		Psychological examination	Date:	Medical	Date:
<b>Status:</b>	Hired	On List	Withdrawn	Disqualified		

---

**B. Name of Agency:**

Position Applied For:

Date Applied:

Address:

City:

State:

Zip:

Background Investigator's Name (if known):

Contact Number, (ext):

Email:

Check each step in the process that you completed, and your status:

<b>Steps:</b>	Application	Written	Physical agility	Oral	Polygraph/CVSA	Background
	Conditional job offer		Psychological examination	Date:	Medical	Date:
<b>Status:</b>	Hired	On List	Withdrawn	Disqualified		

---

**C. Name of Agency:**

Position Applied For:

Date Applied:

Address:

City:

State:

Zip:

Background Investigator's Name (if known):

Contact Number, (ext):

Email:

Check each step in the process that you completed, and your status:

<b>Steps:</b>	Application	Written	Physical agility	Oral	Polygraph/CVSA	Background
	Conditional job offer		Psychological examination	Date:	Medical	Date:
<b>Status:</b>	Hired	On List	Withdrawn	Disqualified		

## SECTION 2: RELATIVES AND REFERENCES

### IMMEDIATE FAMILY

- Provide all applicable information in the spaces below.
- Mark "N/A" if a category is not applicable or if the individual is deceased.

If you need additional space for your answers, attach additional sheets as needed. Be sure to indicate what section number and page this refers.

N/A      **A. Father's Name:** \_\_\_\_\_      D.O.B.: \_\_\_\_\_

Home Address: \_\_\_\_\_

City: \_\_\_\_\_      State: \_\_\_\_\_      Zip: \_\_\_\_\_

Work Address: \_\_\_\_\_

City: \_\_\_\_\_      State: \_\_\_\_\_      Zip: \_\_\_\_\_

Home Phone: \_\_\_\_\_      Cell Phone: \_\_\_\_\_      Work Phone: \_\_\_\_\_

Email: \_\_\_\_\_

N/A      **B. Step-Father's Name:** \_\_\_\_\_      D.O.B.: \_\_\_\_\_

Home Address: \_\_\_\_\_

City: \_\_\_\_\_      State: \_\_\_\_\_      Zip: \_\_\_\_\_

Work Address: \_\_\_\_\_

City: \_\_\_\_\_      State: \_\_\_\_\_      Zip: \_\_\_\_\_

Home Phone: \_\_\_\_\_      Cell Phone: \_\_\_\_\_      Work Phone: \_\_\_\_\_

Email: \_\_\_\_\_

N/A      **C. Mother's Name:** \_\_\_\_\_      D.O.B.: \_\_\_\_\_

Home Address: \_\_\_\_\_

City: \_\_\_\_\_      State: \_\_\_\_\_      Zip: \_\_\_\_\_

Work Address: \_\_\_\_\_

City: \_\_\_\_\_      State: \_\_\_\_\_      Zip: \_\_\_\_\_

Home Phone: \_\_\_\_\_      Cell Phone: \_\_\_\_\_      Work Phone: \_\_\_\_\_

Email: \_\_\_\_\_

N/A      **D. Step-Mother's Name:** \_\_\_\_\_      D.O.B.: \_\_\_\_\_

Home Address: \_\_\_\_\_

City: \_\_\_\_\_      State: \_\_\_\_\_      Zip: \_\_\_\_\_

Work Address: \_\_\_\_\_

City: \_\_\_\_\_      State: \_\_\_\_\_      Zip: \_\_\_\_\_

Home Phone: \_\_\_\_\_      Cell Phone: \_\_\_\_\_      Work Phone: \_\_\_\_\_

Email: \_\_\_\_\_



N/A **E. Spouse/Registered Domestic Partner's Name:**

D.O.B.:

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email: Years of Marriage:

Is there, or has there been, a restraining or stay-away order in effect for this individual? Yes No

N/A **F. Father-in-Law's Name:**

D.O.B.:

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email:

N/A **G. Mother-in-Law's Name:**

D.O.B.:

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email:

N/A **H. Former Spouse/Cohabitant's Name(s):**

D.O.B.: Male Female

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email: Years of Dissolution:

Is there, or has there been, a restraining or stay-away order in effect for this individual? Yes No

N/A I. Former Spouse/Cohabitant's Name(s):

D.O.B.: Male Female

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email: Years of Dissolution:

Is there, or has there been, a restraining or stay-away order in effect for this individual? Yes No

---

**J. BROTHERS AND SISTERS:** List all living siblings, including half-siblings, foster siblings, etc.

N/A 1. Name:

D.O.B.: Male Female

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email:

N/A 2. Name:

D.O.B.: Male Female

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email:

N/A 3. Name:

D.O.B.: Male Female

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email:

N/A 4. Name:

D.O.B.: Male Female

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email:

N/A 5. Name:

D.O.B.: Male Female

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email:

N/A 6. Name:

D.O.B.: Male Female

Home Address:

City: State: Zip:

Work Address:

City: State: Zip:

Home Phone: Cell Phone: Work Phone:

Email:

**K. CHILDREN:** List all of your living children, including natural, adopted, step, and/or foster care. Include any other children who reside with you. Provide the name and contact information of the custodial parent or guardian, if other than you

N/A 1. Name: Male Female

D.O.B.: Custodial parent or guardian (if other than you):

Address:

City: State: Zip:

Contact Number: Email:

N/A      **2. Name:**      Male      Female  
D.O.B.:      Custodial parent or guardian (if other than you):  
Address:  
City:      State:      Zip:  
Contact Number:      Email:

N/A      **3. Name:**      Male      Female  
D.O.B.:      Custodial parent or guardian (if other than you):  
Address:  
City:      State:      Zip:  
Contact Number:      Email:

N/A      **4. Name:**      Male      Female  
D.O.B.:      Custodial parent or guardian (if other than you):  
Address:  
City:      State:      Zip:  
Contact Number:      Email:

N/A      **5. Name:**      Male      Female  
D.O.B.:      Custodial parent or guardian (if other than you):  
Address:  
City:      State:      Zip:  
Contact Number:      Email:

N/A      **6. Name:**      Male      Female  
D.O.B.:      Custodial parent or guardian (if other than you):  
Address:  
City:      State:      Zip:  
Contact Number:      Email:

---

**L. REFERENCES:** List 7-10 people who know you well, such as social and family friends, co-workers, military acquaintances. Do not include relatives, employers, or housemates, or other individuals listed elsewhere.

**1. Name:**      Address:  
City:      State:      Zip:  
Company/Work Address:  
City:      State:      Zip:  
Home Phone:      Work Phone:      Cell Phone:      Email:

How do you know this person (friend, teacher, family, co-worker)?

How long have you known this person?

**2. Name:** \_\_\_\_\_ **Address:** \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Company/Work Address: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Home Phone: \_\_\_\_\_ Work Phone: \_\_\_\_\_ Cell Phone: \_\_\_\_\_ Email: \_\_\_\_\_  
How do you know this person (friend, teacher, family, co-worker)? \_\_\_\_\_  
How long have you known this person? \_\_\_\_\_

**3. Name:** \_\_\_\_\_ **Address:** \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Company/Work Address: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Home Phone: \_\_\_\_\_ Work Phone: \_\_\_\_\_ Cell Phone: \_\_\_\_\_ Email: \_\_\_\_\_  
How do you know this person (friend, teacher, family, co-worker)? \_\_\_\_\_  
How long have you known this person? \_\_\_\_\_

**4. Name:** \_\_\_\_\_ **Address:** \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Company/Work Address: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Home Phone: \_\_\_\_\_ Work Phone: \_\_\_\_\_ Cell Phone: \_\_\_\_\_ Email: \_\_\_\_\_  
How do you know this person (friend, teacher, family, co-worker)? \_\_\_\_\_  
How long have you known this person? \_\_\_\_\_

**5. Name:** \_\_\_\_\_ **Address:** \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Company/Work Address: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
Home Phone: \_\_\_\_\_ Work Phone: \_\_\_\_\_ Cell Phone: \_\_\_\_\_ Email: \_\_\_\_\_  
How do you know this person (friend, teacher, family, co-worker)? \_\_\_\_\_  
How long have you known this person? \_\_\_\_\_

6. Name: \_\_\_\_\_ Address: \_\_\_\_\_  
 City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
 Company/Work Address: \_\_\_\_\_  
 City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
 Home Phone: \_\_\_\_\_ Work Phone: \_\_\_\_\_ Cell Phone: \_\_\_\_\_ Email: \_\_\_\_\_

How do you know this person (friend, teacher, family, co-worker)? \_\_\_\_\_  
 How long have you known this person? \_\_\_\_\_

7. Name: \_\_\_\_\_ Address: \_\_\_\_\_  
 City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
 Company/Work Address: \_\_\_\_\_  
 City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
 Home Phone: \_\_\_\_\_ Work Phone: \_\_\_\_\_ Cell Phone: \_\_\_\_\_ Email: \_\_\_\_\_

How do you know this person (friend, teacher, family, co-worker)? \_\_\_\_\_  
 How long have you known this person? \_\_\_\_\_

8. Name: \_\_\_\_\_ Address: \_\_\_\_\_  
 City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
 Company/Work Address: \_\_\_\_\_  
 City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
 Home Phone: \_\_\_\_\_ Work Phone: \_\_\_\_\_ Cell Phone: \_\_\_\_\_ Email: \_\_\_\_\_

How do you know this person (friend, teacher, family, co-worker)? \_\_\_\_\_  
 How long have you known this person? \_\_\_\_\_

**SECTION 3: EDUCATION**

**NOTE:** You will be required to furnish transcripts or other proof to support all of your educational claims.

Check applicable: High School Diploma GED Discharge documents from armed services with 2 years active duty

**List high schools attended or where you obtained your GED:**

1. Name: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_  
 From: \_\_\_\_\_ To: \_\_\_\_\_ Did you graduate? Yes No  
 2. Name: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_  
 From: \_\_\_\_\_ To: \_\_\_\_\_ Did you graduate? Yes No

**List all colleges or universities attended:**

1. Name: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_  
 From: \_\_\_\_\_ To: \_\_\_\_\_ Type of Degree Earned: \_\_\_\_\_ Total Units Earned: \_\_\_\_\_  
 2. Name: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_  
 From: \_\_\_\_\_ To: \_\_\_\_\_ Type of Degree Earned: \_\_\_\_\_ Total Units Earned: \_\_\_\_\_

3. Name: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_  
 From: \_\_\_\_\_ To: \_\_\_\_\_ Type of Degree Earned: \_\_\_\_\_ Total Units Earned: \_\_\_\_\_

---

**List any trade, vocational, or business schools/institutes attended:**

1. Name: \_\_\_\_\_ From: \_\_\_\_\_ To: \_\_\_\_\_  
 Type of school or training: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_  
 Did you complete the course?      Yes      No

2. Name: \_\_\_\_\_ From: \_\_\_\_\_ To: \_\_\_\_\_  
 Type of school or training: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_  
 Did you complete the course?      Yes      No

3. Name: \_\_\_\_\_ From: \_\_\_\_\_ To: \_\_\_\_\_  
 Type of school or training: \_\_\_\_\_ City: \_\_\_\_\_ State: \_\_\_\_\_  
 Did you complete the course?      Yes      No

---

Have you ever been placed on academic discipline, suspended, or expelled from any high school, college/university, business, or trade school?      Yes      No

If yes, describe in detail below. Starting with high school, list any disciplinary actions received in any school or educational institution. Include when the disciplinary action(s) occurred, name of school(s), and explanation of circumstances.

**SECTION 4: RESIDENCES**

**LIST OF RESIDENCES**

- List all residences during the last ten years or since age 17. Provide complete addresses (include markers such as Street, Drive, Road, East, West, etc., and unit or apartment number). Do not use P.O. Boxes.
- If the residence is a military base, identify the name of the base in the address, nearest city, state, and zip code. DO NOT LIST military barracks mates, unless you shared individual quarters.
- If you need additional space for your answers, attach additional sheets as needed. Be sure to indicate what section number and page this refers to.

**1. Current Residence Address:**

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

If renting; property manager, rent collector, or owner: \_\_\_\_\_ Contact Number: \_\_\_\_\_

Address of property mgr., rent collector, or owner: \_\_\_\_\_ Email: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

From: \_\_\_\_\_ To: \_\_\_\_\_

N/A Name(s) of those with whom you live: \_\_\_\_\_

**2. Former Address:**

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

If renting; property manager, rent collector, or owner: \_\_\_\_\_ Contact Number: \_\_\_\_\_

Address of property mgr., rent collector, or owner: \_\_\_\_\_ Email: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

From: \_\_\_\_\_ To: \_\_\_\_\_

N/A Name(s) of those with whom you live: \_\_\_\_\_

Reason for moving: \_\_\_\_\_

**3. Former Address:**

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

If renting; property manager, rent collector, or owner: \_\_\_\_\_ Contact Number: \_\_\_\_\_

Address of property mgr., rent collector, or owner: \_\_\_\_\_ Email: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

From: \_\_\_\_\_ To: \_\_\_\_\_

N/A Name(s) of those with whom you live: \_\_\_\_\_

Reason for moving: \_\_\_\_\_



**4. Former Address:**

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
If renting; property manager, rent collector, or owner: \_\_\_\_\_ Contact Number: \_\_\_\_\_  
Address of property mgr., rent collector, or owner: \_\_\_\_\_ Email: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
From: \_\_\_\_\_ To: \_\_\_\_\_  
N/A Name(s) of those with whom you live: \_\_\_\_\_  
Reason for moving: \_\_\_\_\_

**5. Former Address:**

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
If renting; property manager, rent collector, or owner: \_\_\_\_\_ Contact Number: \_\_\_\_\_  
Address of property mgr., rent collector, or owner: \_\_\_\_\_ Email: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
From: \_\_\_\_\_ To: \_\_\_\_\_  
N/A Name(s) of those with whom you live: \_\_\_\_\_  
Reason for moving: \_\_\_\_\_

**6. Former Address:**

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
If renting; property manager, rent collector, or owner: \_\_\_\_\_ Contact Number: \_\_\_\_\_  
Address of property mgr., rent collector, or owner: \_\_\_\_\_ Email: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
From: \_\_\_\_\_ To: \_\_\_\_\_  
N/A Name(s) of those with whom you live: \_\_\_\_\_  
Reason for moving: \_\_\_\_\_

**7. Former Address:**

City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
If renting; property manager, rent collector, or owner: \_\_\_\_\_ Contact Number: \_\_\_\_\_  
Address of property mgr., rent collector, or owner: \_\_\_\_\_ Email: \_\_\_\_\_  
City: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_  
From: \_\_\_\_\_ To: \_\_\_\_\_  
N/A Name(s) of those with whom you live: \_\_\_\_\_  
Reason for moving: \_\_\_\_\_

Provide contact information for all housemates listed in the above entries for Section 4 that you have resided with during the past 10 years, or since the age of 17. DO NOT list anyone for whom you have already provided contact information. If you need additional space for your answers, attach additional sheets as needed. Be sure to indicate what section number and page this refers to.

1. Housemate Name: Contact Number: Email:

Current Street Address:

City: State: Zip:

Nature of relationship (friend, relative, landlord, housemate only):

2. Housemate Name: Contact Number: Email:

Current Street Address:

City: State: Zip:

Nature of relationship (friend, relative, landlord, housemate only):

3. Housemate Name: Contact Number: Email:

Current Street Address:

City: State: Zip:

Nature of relationship (friend, relative, landlord, housemate only):

4. Housemate Name: Contact Number: Email:

Current Street Address:

City: State: Zip:

Nature of relationship (friend, relative, landlord, housemate only):

5. Housemate Name: Contact Number: Email:

Current Street Address:

City: State: Zip:

Nature of relationship (friend, relative, landlord, housemate only):

6. Housemate Name: Contact Number: Email:

Current Street Address:

City: State: Zip:

Nature of relationship (friend, relative, landlord, housemate only):

Have you ever been evicted or asked to leave a residence?      Yes      No

Have you ever left a residence owing rent?      Yes      No

If you answered "Yes" to either of the two questions above, explain (include when, where, and circumstances):

## SECTION 5: EXPERIENCE AND EMPLOYMENT

### JOB EXPERIENCE

- Have you EVER served as a Peace Officer, Jailer, or Telecommunicator in another state OR another country?      Yes      No

**If YES, list below.**

- List ALL jobs you have had in the last ten years, including part-time, temporary, self-employment, and volunteer. (Begin with your most current. If more space is needed, continue your response on the additional space page at the end of the Personal History Statement).
- If you have military experience, including reserve duty, enter your military base, assignments, or unit of assignment. Include ALL military services.
- List ALL periods of unemployment in excess of 30 days.

1. Name of Employer or Military Unit:      From:      To:

Address or Base:

City:      State:      Zip:

Supervisor:      Contact Number:      Email:

Job Title:      Reason for Leaving:

Duties/Assignments:

Full-Time      Part-Time      Temporary      Self-Employed      Unemployed

Names of Co-Worker(s) and their Phone Number(s):

Would there be a problem if we contact your current employer?      Yes      No

If yes, explain:

---

### 2. Period of Unemployment

From:      To:

Check if applicable:      Student      Between jobs      Leave of absence      Travel      Other

**3. Name of Employer or Military Unit:**

**From:**

**To:**

Address or Base:

City:

State:

Zip:

Supervisor:

Contact Number:

Email:

Job Title:

Reason for Leaving:

Duties/Assignments:

Full-Time

Part-Time

Temporary

Self-Employed

Unemployed

Names of Co-Worker(s) and their Phone Number(s):

---

**4. Period of Unemployment**

From:

To:

Check if applicable:

Student

Between jobs

Leave of absence

Travel

Other

---

**5. Name of Employer or Military Unit:**

**From:**

**To:**

Address or Base:

City:

State:

Zip:

Supervisor:

Contact Number:

Email:

Job Title:

Reason for Leaving:

Duties/Assignments:

Full-Time

Part-Time

Temporary

Self-Employed

Unemployed

Names of Co-Worker(s) and their Phone Number(s):

---

**6. Period of Unemployment**

From:

To:

Check if applicable:

Student

Between jobs

Leave of absence

Travel

Other

---

7. Name of Employer or Military Unit:

From:

To:

Address or Base:

City:

State:

Zip:

Supervisor:

Contact Number:

Email:

Job Title:

Reason for Leaving:

Duties/Assignments:

Full-Time

Part-Time

Temporary

Self-Employed

Unemployed

Names of Co-Worker(s) and their Phone Number(s):

8. Period of Unemployment

From:

To:

Check if applicable:

Student

Between jobs

Leave of absence

Travel

Other

9. Name of Employer or Military Unit:

From:

To:

Address or Base:

City:

State:

Zip:

Supervisor:

Contact Number:

Email:

Job Title:

Reason for Leaving:

Duties/Assignments:

Full-Time

Part-Time

Temporary

Self-Employed

Unemployed

Names of Co-Worker(s) and their Phone Number(s):

10. Period of Unemployment

From:

To:

Check if applicable:

Student

Between jobs

Leave of absence

Travel

Other

11. Name of Employer or Military Unit:

From:

To:

Address or Base:

City:

State:

Zip:

Supervisor:

Contact Number:

Email:

Job Title:

Reason for Leaving:

Duties/Assignments:

Full-Time

Part-Time

Temporary

Self-Employed

Unemployed

Names of Co-Worker(s) and their Phone Number(s):

12. Period of Unemployment

From:

To:

Check if applicable:

Student

Between jobs

Leave of absence

Travel

Other

13. Name of Employer or Military Unit:

From:

To:

Address or Base:

City:

State:

Zip:

Supervisor:

Contact Number:

Email:

Job Title:

Reason for Leaving:

Duties/Assignments:

Full-Time

Part-Time

Temporary

Self-Employed

Unemployed

Names of Co-Worker(s) and their Phone Number(s):

14. Period of Unemployment

From:

To:

Check if applicable:

Student

Between jobs

Leave of absence

Travel

Other

15. Name of Employer or Military Unit:

From:

To:

Address or Base:

City:

State:

Zip:

Supervisor:

Contact Number:

Email:

Job Title:

Reason for Leaving:

Duties/Assignments:

Full-Time

Part-Time

Temporary

Self-Employed

Unemployed

Names of Co-Worker(s) and their Phone Number(s):

16. Period of Unemployment

From:

To:

Check if applicable:

Student

Between jobs

Leave of absence

Travel

Other

17. Name of Employer or Military Unit:

From:

To:

Address or Base:

City:

State:

Zip:

Supervisor:

Contact Number:

Email:

Job Title:

Reason for Leaving:

Duties/Assignments:

Full-Time

Part-Time

Temporary

Self-Employed

Unemployed

Names of Co-Worker(s) and their Phone Number(s):

18. Have you ever been disciplined at work? (This includes written warnings, formal letters of reprimands, suspensions, reductions in pay, reassignments, or demotions). Yes No

19. Have you ever been fired, released from probation, or asked to resign from any place of employment? Yes No

20. Were you ever involved in a physical/verbal altercation with a supervisor, co-worker, or customer? Yes No

21. Have you ever resigned without giving two weeks-notice? Yes No

22. Have you ever resigned in lieu of termination? Yes No

23. Have you ever been accused of discrimination (such as sexual harassment, racial bias, sexual orientation harassment, etc.) by a co-worker, superior, subordinate, and/or customer? Yes No

24. Were you ever the subject of a written complaint at work?      Yes      No
25. Have you ever been counseled at work due to lateness or absences?      Yes      No
26. Did you ever receive an unsatisfactory performance review?      Yes      No
27. Have you ever sold, released, or given away legally confidential information?      Yes      No
28. Have you ever called in sick when you were neither sick nor caring for a sick family member?      Yes      No

If yes, how many sick days have you used in the past five years which were not due to illness?

If you answered "Yes" to any of Questions 18 – 28 (at the bottom of the previous page and above), explain (include when, where, and circumstances; indicate the corresponding question number):

---

Has your work performance ever been affected by your use of alcohol or drugs?      Yes      No

When?      Name of Employer:

In the past ten years, have you been warned by an employer about your drinking or drug habits and their impact on your performance?      Yes      No

When?      Name of Employer:

## SECTION 6: MILITARY EXPERIENCE

(Complete for all branches of the military served. Add pages if necessary).

1. Are you required to register for the Selective Service?      Yes      No

2. If yes, have you registered?      Yes      No

If no, explain:

Branch of Service:

Dates Served From:

To:

Type of Discharge:      Entry Level      Honorable      General      Other than Honorable

Re-entry Code (1 – 4) if applicable; refer to your DD-214:

3. Are you currently participating in one of the following?      Military Reserve      National Guard

If checked, date obligation ends:

4. Have you ever been the subject of any judicial or non-judiciary disciplinary action (such as, court martial, captain's mast, office hours, company punishment)?      Yes      No



5. Were you ever denied a security clearance, or had a clearance revoked, suspended or downgraded, either military or any other federal, state, or municipal clearance?      Yes      No

If you answered "Yes" to either of the last two questions (questions 4 and 5), explain. Include dates and circumstances.

## SECTION 7: FINANCIAL

### INCOME AND EXPENSES:

For each of the following questions, fill in the amounts to the nearest dollar.

1. From your employer(s), what is your monthly income?

2. Do you have income other than from your salary or wages?      Yes      No

If yes, fill in amount:                      per month      Explain:

3. Approximately how much do you spend each month? (Estimate your monthly living expenses, include housing, utilities, credit cards or other loan payments, food, gas and car maintenance, entertainment, etc., as well as any other obligations you may have).

4. Have you ever filed for or declared bankruptcy (Chapter 7, 11 or 13)?      Yes      No

5. Have any of your bills ever been turned over to a collection agency?      Yes      No

6. Have you ever had purchased goods repossessed?      Yes      No

7. Have your wages ever been garnished?      Yes      No

8. Have you ever been delinquent on income or other tax payments?      Yes      No

9. Have you ever failed to file income tax or cheated/lie on an income tax form?      Yes      No

10. Have you ever had an employment bond refused?      Yes      No

11. Have you ever avoided paying any lawful debt by moving away?      Yes      No

12. Have you ever defaulted on a loan, including a student loan?      Yes      No

13a. Have you ever borrowed money to pay for a gambling debt?      Yes      No

13b. If "Yes," do you currently have any outstanding debts as a result of gambling?      Yes      No

14. Have you ever spent money for illegal purposes (e.g., illegal drugs, prostitution, purchase fraudulent documents, etc.)?  
Yes      No

15. Have you ever failed to make or been late on a court-ordered payment e.g., child support, alimony, restitution, etc.)?  
Yes      No

16. Have you written three or more bad checks in a one-year period?      Yes      No



5. Have you ever been placed on court probation as an adult?      Yes      No
6. Have you ever been convicted of any charge that would prevent you from legally possessing a firearm or ammunition?  
Yes      No
7. Were you ever required to appear before a juvenile court for an act which would have been a crime, if committed as an adult?      Yes      No
8. Have you ever been a party in a civil lawsuit (e.g., small claims actions, dissolutions, child custody, paternity, support, etc.)?  
Yes      No
9. Have the police ever been called to your home for any reason?      Yes      No
10. Have you or your spouse/partner ever been referred to Child Protective Services?      Yes      No
11. Have you ever been the subject of an emergency protective, restraining, or stay-away order?      Yes      No
12. Have you settled any civil suit in which you, your insurance company, or anyone else on your behalf was required to make payment to the other party?      Yes      No
13. Have you ever fraudulently received welfare, unemployment compensation, compensation, or other state or federal assistance?      Yes      No
14. Have you ever filed a false insurance or workers' compensation claim?      Yes      No

If you answered "Yes" to any of Questions 5 – 14 (above), explain. Include court case or document, dates, and circumstances. Indicate the corresponding question number:

---

### Undetected Acts – Part 1

Within the past **seven** years **OR** at any time after you were first employed in law enforcement, have you ever committed any of the following misdemeanors?

15. Annoying/obscene phone calls      Yes      No
16. Assault (use of force or violence upon another)      Yes      No
17. Assault on a family member (use of force or violence upon a family member)      Yes      No
18. Brandishing a weapon (any type of weapon)      Yes      No
19. Carrying a concealed weapon without a permit      Yes      No
20. Contributing to the delinquency of a minor      Yes      No
21. Defrauding an innkeeper (not paying for food or room at a hotel/motel)      Yes      No
22. Driving under the influence of alcohol and/or drugs      Yes      No

23. Drunk in public (being so intoxicated in a public place that you're not able to care for yourself)      Yes      No
24. Hit and run collision (no injuries)      Yes      No
25. Hunting or fishing without a license      Yes      No
26. Illegal gambling      Yes      No
27. Impersonating a peace officer      Yes      No
28. Indecent exposure (including flashing or mooning)      Yes      No
29. Joyriding (using a car or other vehicle without owner's permission)      Yes      No

**Undetected Acts – Part 1**

At any time in your life, have you **ever** committed any of the following?

30. Arson (intentionally destroying property by setting a fire)      Yes      No
31. Assault with a deadly weapon      Yes      No
32. Theft of a vehicle and/or vehicle parts      Yes      No
33. Burglary (entering a structure or vehicle to commit theft or other crime)      Yes      No
34. Child molestation (performing unlawful acts with a child)      Yes      No
35. Accessing, producing, or possessing child pornography      Yes      No
36. Injury to a child, elderly, and/or disabled      Yes      No
37. Embezzlement (theft of money or other valuables entrusted to you)      Yes      No
38. Felony drunk driving (involving injuries)      Yes      No
39. Forcible rape or other act of unlawful intercourse/sexual activity      Yes      No
40. Forgery (falsifying any type of document, check certificate, license, currency, etc.)      Yes      No
41. Hit and run (with injuries)      Yes      No
42. Hate crime      Yes      No
43. Insurance fraud      Yes      No
44. Theft (value of over \$500 and/or any firearm)      Yes      No
45. Murder, homicide, or attempted murder      Yes      No
46. Perjury (lying under oath)      Yes      No
47. Possession of an explosive/destructive device      Yes      No
48. Robbery (theft from another person using a weapon, force, or fear)      Yes      No
49. Stalking      Yes      No
50. Blackmail or extortion      Yes      No
51. Any other act amounting to a felony      Yes      No

If you answered "YES" to **any** of the Questions 15 – 51 (on the previous two pages), fully explain circumstances, including dates, names of individuals involved, and resolution. Indicate the corresponding question number for each explanation.

---

Questions about your current and past recreational drug use. This covers the use of **any** drug, including the unauthorized use of prescription drugs. Your answers should include, **but not limited to**, your use of any of the following drugs.

- |   |                            |
|---|----------------------------|
| Amphetamines/Methamphetamine Uppers, Speed, Crank, etc. | Heroin/Opium               |
| Barbiturates (Downers)                                  | Marijuana                  |
| Cocaine/Crack Cocaine                                   | Mescaline                  |
| Designer Drugs (Ecstasy, Synthetic Heroin, etc.)        | Morphine                   |
| GHB (Date Rape Drug)                                    | PCP/Angel Dust             |
| Glue  | Quaaludes                  |
| Hallucinogens (Peyote, LSD, Mushrooms)                  | Steroids                   |
| Hashish/Hashish Oil                                     | Tetrahydrocannabinol (THC) |

**52. Within the past three years**, have you used any non-prescribed drug(s) as indicated above or unauthorized prescription drugs?      Yes      No

If yes, give details, including drug(s) used and circumstances:

---

**53. Prior to the past three years (check all that apply):**

I have never used any drug recreationally.

I have tried or used one or more drugs listed above, but only under limited circumstances (for example: experimentation, at parties, concerts, special events, etc.).

If you have, give details including drug(s) used, most recent date used, and circumstances:

Have you **ever** engaged in any of the activities listed below for drugs, narcotics, or illegal substances – including marijuana?

Sold          Manufactured          Purchased          Furnished          Cultivated          Carried or held for another

If you checked any of the items above, give details including drug(s) involved, over what time period(s), and circumstances:

---

**SECTION 9: MOTOR VEHICLE OPERATION**

Current Driver License #:                                  State of Issue:                                  Expiration Date:

Full name under which license was granted:

**List other states where you have been licensed to operate a motor vehicle:**

1.    N/A    State of Issue:                                  Type of License:                                  License Number:

Name under which license was granted:

2.    N/A    State of Issue:                                  Type of License:                                  License Number:

Name under which license was granted:

3.    N/A    State of Issue:                                  Type of License:                                  License Number:

Name under which license was granted:

---

Have you ever been refused a driver’s license by any state?                  Yes                  No

If yes, explain (include when, where, and circumstances):

---

Has your driver’s license ever been suspended or revoked?                  Yes                  No

If yes, explain (include when, where, and circumstances):

**List your current liability insurance on your vehicle(s):**

4. Type of Coverage:      Insured                      Bonded                      Cash Deposit  
Vehicle Make/Model:                                      Year:                                      Vehicle License:  
Insurance Company:                                      Policy Number:                                      Expires:  
Address:  
City:                                      State:                                      Zip:                                      Contact Number:

5. Type of Coverage:      Insured                      Bonded                      Cash Deposit  
Vehicle Make/Model:                                      Year:                                      Vehicle License:  
Insurance Company:                                      Policy Number:                                      Expires:  
Address:  
City:                                      State:                                      Zip:                                      Contact Number:

6. Type of Coverage:      Insured                      Bonded                      Cash Deposit  
Vehicle Make/Model:                                      Year:                                      Vehicle License:  
Insurance Company:                                      Policy Number:                                      Expires:  
Address:  
City:                                      State:                                      Zip:                                      Contact Number:

7. Type of Coverage:      Insured                      Bonded                      Cash Deposit  
Vehicle Make/Model:                                      Year:                                      Vehicle License:  
Insurance Company:                                      Policy Number:                                      Expires:  
Address:  
City:                                      State:                                      Zip:                                      Contact Number:

---

**List all traffic citations, excluding parking citations, that you have received within the past seven years:**

8. Nature of Violation:  
Location (Street, City, State, Zip):  
Date Violation Occurred:                      Action Taken:      Not Guilty                      Fined                      Traffic School                      Dismissed

**9. Nature of Violation:**

Location (Street, City, State, Zip):

Date Violation Occurred:                      Action Taken:    Not Guilty            Fined            Traffic School            Dismissed

**10. Nature of Violation:**

Location (Street, City, State, Zip):

Date Violation Occurred:                      Action Taken:    Not Guilty            Fined            Traffic School            Dismissed

Has a traffic citation ever resulted in a warrant or caused your driver's license to be withheld due to any of the following? (Check all that apply).

Failed to appear                      Failed to complete traffic school                      Failed to pay the required fine

If checked, explain circumstances:

Have you been involved as the driver in a motor vehicle accident within the past seven years?                      Yes                      No

**If yes, give details:**

**11. Date:**                      Location (Street, City, State, Zip):

Police Report?    Yes            No                      Injury or Non-Injury?    Injury            Non-Injury

Law Enforcement Agency:

**12. Date:**                      Location (Street, City, State, Zip):

Police Report?    Yes            No                      Injury or Non-Injury?    Injury            Non-Injury

Law Enforcement Agency:

**13. Date:**                      Location (Street, City, State, Zip):

Police Report?    Yes            No                      Injury or Non-Injury?    Injury            Non-Injury

Law Enforcement Agency:

**14. Date:**                      Location (Street, City, State, Zip):

Police Report?    Yes            No                      Injury or Non-Injury?    Injury            Non-Injury

Law Enforcement Agency:





**SECTION 10: SOCIAL MEDIA SITES**

Have you ever had a social media site (i.e. Facebook, My Space, Instagram, Snapchat etc.)?      Yes      No

List all social media sites, blogs, and/or websites you have created. Provide the website URL and your username.

## SECTION 11: ADDITIONAL SPACE

- Duplicate this page as needed to include additional information that does not fit elsewhere on this form (e.g., additional family members, schools, residences, employers, explanations to questions, etc.).
- Identify the corresponding section, question number, and specific item being referenced.

**SECTION 12: CERTIFICATION**

I hereby certify that I have personally completed and initialed each page of this form and any supplemental page(s) attached, and that all statements made are true and complete to the best of my knowledge and belief. I understand that any misstatement of material fact may subject me to disqualification; or, if I have been appointed, may disqualify me from continued employment.

\_\_\_\_\_  
Signature of Applicant

\_\_\_\_\_  
Date

Sworn to and subscribed before me, this the \_\_\_\_\_ day of \_\_\_\_\_, \_\_\_\_\_.

Notary public in and for, State of \_\_\_\_\_.

My commission expires: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_.

\_\_\_\_\_  
Printed Name of Notary

\_\_\_\_\_  
Signature of Notary

Notary Seal or Stamp:

TEAGUE POLICE DEPARTMENT

Photographic Line-up Form

Case Number: \_\_\_\_\_

Admonition. Read the following to the witness:

1. You will be shown a number of photographs.
2. I have been asked to show these photographs to you, but I do not know the identity of the perpetrator.
3. These photographs are numbered, and I will show them one at a time, in a random order. Please take as much time as you need before moving to the next photograph.
4. All of the photographs will be shown even if you make an identification.
5. The person who committed the crime *may or may not* be in this line-up and you should not feel compelled to choose anyone.
6. Regardless of whether you make an identification, we will continue to investigate this incident.
7. If you recognize anyone, please tell me which photograph you recognize and how or why you recognize the individual.
8. You should not discuss the identification procedure or its results with other eyewitnesses involved in the case and should not speak with the media regarding any identification you may make.
9. If you make an identification, I am required to ask you to state in your own words how certain you are of the identification.

I, \_\_\_\_\_, understand the above information.

Line-up administrator: \_\_\_\_\_ Order of photographs shown: \_\_\_\_\_

**Statement of Victim/Witness:**

On the \_\_\_ day of \_\_\_\_\_, 20\_\_\_, at \_\_\_ o'clock \_\_m), I viewed a photo line-up. This line-up contained photographs of \_\_\_\_\_persons.

I did identify the person with the number \_\_\_\_\_.

Identification comments / Level of certainty:

\_\_\_\_\_  
\_\_\_\_\_.

Viewer's signature: \_\_\_\_\_

I was unable to positively identify any of the persons in the line-up.

Viewer's signature: \_\_\_\_\_.

Other persons in attendance during line-up, including any translator if used:

Name and address: \_\_\_\_\_

Name and address: \_\_\_\_\_

**TEAGUE POLICE DEPARTMENT**

**Photographic Line-up Form**

Case Number: \_\_\_\_\_

**Read the following to the witness:**

1. You will be advised of the procedures for viewing in a field identification.
2. The fact that an individual is being shown to you should not cause you to believe or guess that the guilty person(s) has been identified or arrested.
3. This *may or may not* be the person who committed the crime.
4. You are in no way obligated to identify anyone. It is as important to clear the innocent as it is to identify the guilty.
5. Regardless of whether you make an identification, the police will continue to investigate this incident.
6. If you recognize anyone, please tell me how you recognize the individual.
7. We are required to ask you to state in your own words how certain you are of any identification.

I, \_\_\_\_\_, understand the above information.

I understand the need to describe my level of certainty regarding identification and after viewing the person(s) shown have identified him/her/them as \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Viewer's Signature: \_\_\_\_\_

Officer's printed name: \_\_\_\_\_

Officer's signature: \_\_\_\_\_

Other persons in attendance during field identification.

Name and Address: \_\_\_\_\_

Name and Address: \_\_\_\_\_



**CITY OF TEAGUE POLICE DEPARTMENT  
PUBLIC RECORDS REQUEST FORM**

**DEPARTAMENTO DE POLICÍA DE LA CIUDAD DE  
TEAGUE  
FORMULARIO DE SOLICITUD DE REGISTROS  
PÚBLICOS**

ALL REQUESTS MUST BE IN WRITING AND DELIVERED BY E-MAIL TO teaguepolice@cityofteaguetx.com; OR FAX TO 254-739-3213; OR BY MAIL TO Teague Police Department 315 Main Street, Teague, TX 75860. (TODAS LAS SOLICITUDES DEBEN SER ESCRITAS Y ENTREGADAS POR CORREO ELECTRÓNICO A teaguepolice@cityofteaguetx.com; O FAX A 254-739-3213; O POR CORREO A Teague Police Department 315 Main Street, Teague, TX 75860.)

**NAME OF REQUESTER (Nombre del solicitante):** \_\_\_\_\_

**MAILING ADDRESS (DIRECCIÓN DE ENVÍO):** \_\_\_\_\_

**TELEPHONE AND/OR FAX NO. (Teléfono y/o Fax #):** \_\_\_\_\_

**E-MAIL ADDRESS (DIRECCIÓN DE CORREO ELECTRÓNICO):**  
\_\_\_\_\_

**SIGNATURE OF REQUESTER (Firma del requisito):** \_\_\_\_\_

**DATE (Fecha):** \_\_\_\_\_

Pursuant to the Public Information Act, Texas Government Code, Section 552, I hereby request the following information currently existing in the records of the City of Teague Police Department, Texas (De conformidad con la Ley de Información Pública, Código de Gobierno de Texas, Sección 552, solicito la siguiente información que existe actualmente en los registros del Departamento de Policía de la Ciudad de Teague, Texas):

List information as specifically as possible, including names, dates and case numbers, if known. Attach a separate sheet to this form if necessary. \*\*If requesting an ACCIDENT/CRASH Report, please complete page

2 of this request form. (Enumere la información lo más específicamente posible, incluidos nombres, fechas y números de casos, si los conoce. Adjunte una hoja separada a este formulario si es necesario. \*\* Si solicita un informe ACCIDENT / CRASH, complete la página 2 de este formulario de solicitud.)

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(Check one) A. \_\_\_\_\_ I request copies (charged per TAC guidelines)(Yo solicito de copias (cargada por TAC directrices)

(Marque Uno) B. \_\_\_\_\_ I request only to view records (Yo Solo solicito ver registros)

C. \_\_\_\_\_ Other (please explain) Otro (por favor explique)

In making this request, I understand the City is under no obligation to create a document to satisfy my request or to comply with a standing request for information. I further understand that the information will be released only in accordance with the Public Information Act, which may require a determination as to confidentiality by the Texas Attorney General prior to release. I further understand the information will be promptly released or the requestor will be notified in writing within 10 days after the request is submitted. (Al formular esta petición, entiendo que la ciudad no tiene la obligación de crear un documento para satisfacer mi petición o para cumplir con una solicitud de información permanente. Yo entiendo que la información será liberado sólo en conformidad con la Ley de Información Pública, lo que puede requerir una decisión en cuanto a la confidencialidad por el Procurador General de Texas antes de la liberación. Además, entiendo la información será puesto en libertad de inmediato o el solicitante será notificado por escrito dentro de los 10 días después del envío de la solicitud.)

**City Use Only (Uso de la ciudad solamente)**

Date received: \_\_\_\_\_ Employee receiving information: \_\_\_\_\_

Date/Dept. Forwarded to, if Applicable: \_\_\_\_\_

Date released: \_\_\_\_\_ Amount charged: \_\_\_\_\_

Miscellaneous comments/instructions: \_\_\_\_\_



CITY OF TEAGUE POLICE DEPARTMENT  
ACCIDENT REPORT REQUEST  
DEPARTAMENTO DE POLICÍA DE LA CIUDAD  
DE TEAGUE

*Reporte de accidente solicitar*

Texas Transportation Code §550.065(c)(4) limits the release of a crash report to any person directly concerned in the accident or having a proper interest therein. Please provide photo identification and any supporting documentation to verify your status as a qualified individual. *(Código de Transporte de Texas §550.065(c)(4) limita la publicación de un informe de fallo a toda persona directamente interesada en el accidente o tener un adecuado interés en ellos. Sírvase proporcionar una identificación con foto y toda la documentación acreditativa para verificar su estado como un individuo calificado.)*

*"By signing below, I certify that I meet the requirements of Texas Transportation Code §550.065(c)(4), and am authorized by law to obtain a copy of the requested crash report based on the following qualification: ("Por la firma a continuación, certifico que cumpla con los requisitos del Código de Transporte de Texas §550.065(c)(4), y estoy autorizado por la ley para obtener una copia de la solicitud de informe de fallo basado en la calificación siguiente:)*

\_\_\_\_\_ **A person involved in the accident** *(Una persona involucrada en el accidente)*

\_\_\_\_\_ **The authorized representative of any person involved in the accident** *(El representante autorizado de cualquier persona involucrada en el accidente)*

\_\_\_\_\_ **A driver involved in the accident** *(Un conductor implicado en el accidente)*

\_\_\_\_\_ **An employer, parent, or legal guardian of a driver involved in the accident** *(Un empleador, padre o tutor legal de un conductor implicado en el accidente)*

\_\_\_\_\_ **The owner of a vehicle or property damaged in the accident** *(El propietario de un vehículo o propiedad dañada en el accidente)*

\_\_\_\_\_ **A person who has established financial responsibility for a vehicle involved in the accident in a manner described in Section 601.051, including a policyholder of a motor vehicle liability insurance policy covering the vehicle** *(Una persona que ha establecido la responsabilidad financiera por un vehículo implicado en el accidente, en la forma descrita en la Sección 601.051, incluyendo un asegurado de una póliza de seguro de responsabilidad civil de los vehículos de motor que cubre el vehículo)*

\_\_\_\_\_ **An insurance company that issued an insurance policy covering a vehicle involved in the accident** *(Una compañía de seguros que emitió una póliza de seguros que cubra un vehículo implicado en el accidente)*

\_\_\_\_\_ **An insurance company that issued an insurance policy covering any person involved in the accident** *(Una compañía de seguros que emitió una póliza de seguros que cubra cualquier persona involucrada en el accidente)*

\_\_\_\_\_ **A person under contract to provide claims or underwriting information to a person** *(Una persona bajo contrato para proporcionar información de suscripción o reclamaciones a una persona)*

\_\_\_\_\_ **A radio or television station that holds a license issued by the Federal Communications Commission** *(Una estación de radio o televisión que posee una licencia expedida por la Comisión Federal de Comunicaciones)*

\_\_\_\_\_ **A newspaper that is a free newspaper of general circulation or qualified under Section 2051.044, Government Code, to publish legal notices, published at least once a week, and available and of interest to the general public in connection with the dissemination of news**

*(Un periódico que es un periódico gratuito de circulación general o calificado bajo la sección 2051.044 del Código de Gobierno, para publicar avisos legales, publicados por lo menos una vez a la semana, y disponibles, y de interés para el público en general en relación con la difusión de noticias)*

\_\_\_\_\_ **A person who may sue because of death resulting from the accident** *(Una persona que puede demandar a causa de la muerte resultantes del accidente)*

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**Providing false information on this governmental record is a violation of Texas Penal Code §37.10 and could result in criminal penalties.**

*In the 84<sup>th</sup> R legislative session (2015), §550.065 was amended. Previously, the law stated that a governmental entity could release an accident report to anyone that could provide two or more of the following: 1) the date of the accident, 2) the specific address of the highway or street where the accident occurred; or 3) the name of any person involved in the accident. Current law now prohibits governmental entities from releasing accident reports to persons with no connection to the accident, and provides the list of authorized individuals as shown above.*



# Teague Police Department

## PROPERTY - EVIDENCE ROOM INSPECTION REPORT

Date: \_\_\_\_\_ Property Custodian: \_\_\_\_\_

Inspector Name: \_\_\_\_\_ Rank/Position: \_\_\_\_\_

Inspection process requires Inspector to review of Property and Evidence handling procedures prior to Inspection and detailed inspection of property and evidence handling to ensure compliance with those procedures. Inspections conducted at least bi-annually.

Written Property and Evidence Procedures Reviewed:                      Y   N   Date: \_\_\_\_\_

1. Is Property Room maintained in a secure manner? Y      N  
Comments: \_\_\_\_\_
2. Is the alarm system working as intended (if so equipped)? Y      N  
Comments: \_\_\_\_\_ Last Tested: \_\_\_\_\_
3. Is sign-in log being utilized and properly completed? Y      N  
Comments: \_\_\_\_\_
4. Review recent Property submissions by officers. Is property being submitted properly? Y      N  
Comments: \_\_\_\_\_
5. Observe Property Custodian process one item from receipt to storage. Were proper procedures followed? Y      N  
Comments: \_\_\_\_\_
6. Locate a property item identified for disposal. Were proper procedures followed, including disposal authority and paperwork? Y      N  
Comments: \_\_\_\_\_
7. Is the property room clean, free from trash, and all property and evidence properly processed and stored? (No Backlog) Y      N
8. Is property being processed for disposal in a timely manner? Y      N  
Last property disposal date: \_\_\_\_\_ Next: \_\_\_\_\_  
Comments: \_\_\_\_\_
9. Select at least one item of property from the listed categories below, review the property and evidence paperwork and request the item be located. Determine if property is properly packaged, processed, and properly stored/located.

Item Type	Report/Invoice#	Pkg'd Properly	Processed	Stored	Located	Comment
Money	_____	_____	_____	_____	_____	_____
Jewelry	_____	_____	_____	_____	_____	_____
Handgun	_____	_____	_____	_____	_____	_____
Long Gun	_____	_____	_____	_____	_____	_____
Random	_____	_____	_____	_____	_____	_____
Comments:	_____					

**Inspector Signature:** \_\_\_\_\_

**Date:** \_\_\_\_\_



# Teague Police Department

315 Main Street

Teague, Texas 75860

Phone: (254) 739-2553 Fax: (254) 739-3213

DeWayne Philpott, Chief of Police

## Receipt for Child

\_\_\_\_\_  
Date Released

\_\_\_\_\_  
Time Released

\_\_\_\_\_  
Full Name of Child

\_\_\_\_\_  
Address

\_\_\_\_\_  
Age

\_\_\_\_\_  
Sex

\_\_\_\_\_  
D.O.B.

The above-named child was taken into custody by the undersigned for the offense of \_\_\_\_\_, which is alleged to have occurred on the \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_\_, at \_\_\_\_\_ o'clock \_\_\_\_\_M. at \_\_\_\_\_.

\_\_\_\_\_  
Officer's Signature and Badge #

It is important that the undersigned clearly understands the terms of this release. It is in no way to be interpreted as a final disposition. It is further understood that upon request of the court or official of the court, the said Child will be promptly returned to the designated place.

The undersigned acknowledges receipt of a copy of this notice and that the above-named child was released on this date to the undersigned.

\_\_\_\_\_  
Parent/Guardian/Custodian (Printed Name)

\_\_\_\_\_  
Parent/Guardian/Custodian (Signature)

\_\_\_\_\_  
Address

\_\_\_\_\_  
City / State / Zip

\_\_\_\_\_  
Telephone Number(s)

***Honesty, Integrity, Pride***



# Teague Police Department

315 Main Street

Teague, Texas 75860

Phone: (254) 739-2553 Fax: (254) 739-3213

**DeWayne Philpott, Chief of Police**

## *Receipt of Criminal Cases*

**DATE :** \_\_\_\_\_

Case Number	Charge	Defendant Name

I, \_\_\_\_\_ of the Freestone County Attorney's  
PRINT NAME  
 Office, received the above listed cases, which include Criminal History  
 Printouts, on this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_.

\_\_\_\_\_  
 signature

\_\_\_\_\_  
 print name



# Teague Police Department

315 Main Street

Teague, Texas 75860

Phone: (254) 739-2553 Fax: (254) 739-3213

**DeWayne Philpott, Chief of Police**

---

CASE: \_\_\_\_\_

I, \_\_\_\_\_, RECEIVED THE FOLLOWING PROPERTY:

---

---

---

---

---

THE ABOVE WAS RELEASED BY FOLLOWING PERSON:

NAME: \_\_\_\_\_

DOB: \_\_\_\_\_

DL: \_\_\_\_\_

ADDRESS: \_\_\_\_\_

\_\_\_\_\_

PH#: \_\_\_\_\_

WK#: \_\_\_\_\_

RELEASED BY: \_\_\_\_\_

DATE: \_\_\_\_\_



# Teague Police Department

315 Main Street

Teague, Texas 75860

Phone: (254) 739-2553 Fax: (254) 739-3213

DeWayne Philpott, Chief of Police

---

## *Receipt of Warrant*

DATE : \_\_\_\_\_


I, \_\_\_\_\_ of the Freestone County

PRINT NAME

Sheriff's Office, received the above listed warrant, which includes complaint/affidavit, on this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_.

\_\_\_\_\_  
signature

\_\_\_\_\_  
print name



# DISPOSITION SHEET

Arresting Officer: \_\_\_\_\_

## INSTRUCTIONS

**REASON FOR THIS FORM.** The U. S. Supreme Court has ruled that unless a disposition is shown for an arrest and the charge, then that arrest must be DELETED from the Subject's record and transcript.

The OFFICER who files charges and prepares the necessary follow up report will PREPARE A DISPOSITION SHEET. The information requested in the upper portion is ESSENTIAL. It MUST be completed in detail.

The OFFICER delivering the Offense Report and any Supplement Reports to the City Attorney, County Attorney or District Attorney will make certain that a complete Disposition Sheet is included with the reports.

The CITY or COUNTY or DISTRICT ATTORNEY, for REASONS stated in paragraph one, are **URGED** to complete their portion of the form and return immediately after Court Disposition.

<b>DISPOSITION SHEET</b>		<b>RETURN TO: TEAGUE POLICE DEPARTMENT</b>			
<b>Defendant's Name:</b> _____ (Last, First, Middle)		<b>Race:</b> _____	<b>Sex:</b> _____	<b>Age:</b> _____	<b>Date of Birth:</b> _____
<b>Case File Number:</b> _____	<b>Offense Date:</b> _____	<b>Offense Number:</b> _____	<b>Warrant Number:</b> _____	<b>Capias Number:</b> _____	
<b>CHARGES FILED</b>					
1. _____					
2. _____					
3. _____					
4. _____					

<b>PROSECUTOR:</b> District Attorney		<b>Cause Number:</b> _____	
<b>PLEA:</b> Nolo Contenders <input type="checkbox"/> Not Guilty <input type="checkbox"/> Guilty <input type="checkbox"/>		<b>SENTENCED IN:</b>	
<b>TRIAL RESULTS:</b> Not Guilty <input type="checkbox"/> Guilty <input type="checkbox"/>		<input type="checkbox"/> Justice Court, Precinct No. _____ Place _____	
		<input type="checkbox"/> County Court (at Law)	
		<input type="checkbox"/> _____ District Court	
		<input type="checkbox"/> _____ County Court	
		Trial Judge: _____	
<b>CHARGES:</b> Same as Above <input type="checkbox"/> Reduced to: <input type="checkbox"/>			
1. _____			
2. _____			
3. _____			

<p style="text-align: center;"><b>DISPOSITION(s)</b></p> <p style="text-align: center;">(If more than one, indicate for which charge)</p> <p><input type="checkbox"/> NO BILLED</p> <p><input type="checkbox"/> CASE PRESENTED-PROSECUTION REFUSED</p> <p><input type="checkbox"/> DISMISSED AT TIME OF EXAMINING TRIAL</p> <p><input type="checkbox"/> DISMISSED</p> <p><input type="checkbox"/> _____ YEAR(s) TDCJ-ID, or TDCJ- State Jail AND / OR \$ _____ FINE.</p> <p><input type="checkbox"/> CONCURRENT WITH OTHER</p> <p><input type="checkbox"/> CONSECUTIVE WITH OTHER</p>	<p style="text-align: center;"><b>Probation</b></p> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/> <hr/>
---	---

REMARKS: \_\_\_\_\_  
\_\_\_\_\_

DISPOSITION DATE: \_\_\_\_\_  
SIGNATURE OF PERSON COMPLETING DISPOSITION: \_\_\_\_\_

# TEAGUE POLICE DEPARTMENT - STRANGULATION SUPPLEMENT

## TO BE COMPLETED IN ADDITION TO **OFFENSE** REPORT

CASE # \_\_\_\_\_ DATE OF ASSAULT \_\_\_\_\_ TODAY'S DATE \_\_\_\_\_

**VICTIM INFORMATION**  
TO BE COMPLETED BY POLICE OFFICER

Victim's Name (last, first, middle) \_\_\_\_\_ DOB \_\_\_\_\_

- ◆ Method and/or Manner (how was Victim strangled)  One Hand - R  One Hand - L  Two Hands  Forearm  
 Knee/Foot  Chokehold  Other (explain) \_\_\_\_\_
- ◆ Is the Suspect right or left handed?  Right Handed  Left Handed
- ◆ Estimate how long you were strangled \_\_\_\_\_ Minute(s) \_\_\_\_\_ Second(s) Multiple times?  Yes # \_\_\_\_\_  No
- ◆ Suffocated?  Yes  No \_\_\_\_\_ Minute(s) \_\_\_\_\_ Second(s) What was used? \_\_\_\_\_
- ◆ What did suspect say during strangulation/suffocation? \_\_\_\_\_
- ◆ Describe Suspect's demeanor during strangulation/suffocation? \_\_\_\_\_
- ◆ Describe how Suspect's face looked during strangulation/suffocation? \_\_\_\_\_
- ◆ What made Suspect stop? \_\_\_\_\_
- ◆ What did Victim think was going to happen during strangulation/suffocation? \_\_\_\_\_
- ◆ Has Suspect strangled/suffocated you before?  Yes # \_\_\_\_\_  No

Estimate Pressure Used (check) 1 2 3 4 5 6 7 8 9 10 (1=WEAK - 10=EXTREMELY STRONG)

VICTIM'S SYMPTOMS TO BE COMPLETED BY POLICE OFFICER				
SYMPTOMS	DURING	AFTER	VOICE CHANGES	SWALLOWING CHANGES
unable to breathe	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> painful to speak	<input type="checkbox"/> neck tenderness
difficult to breathe	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> raspy/hoarse voice	<input type="checkbox"/> trouble swallowing
physical pain	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> coughing	<input type="checkbox"/> painful to swallow
rapid breathing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> unable to speak	<input type="checkbox"/> neck pain
shallow breathing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> whispering	<input type="checkbox"/> Other (explain below)
coughing up blood	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Other (explain below)	
nausea	<input type="checkbox"/>	<input type="checkbox"/>	<b>Explain other:</b> _____	
vomiting/dry heaving	<input type="checkbox"/>	<input type="checkbox"/>		
dizziness	<input type="checkbox"/>	<input type="checkbox"/>		
headache	<input type="checkbox"/>	<input type="checkbox"/>		
feel faint	<input type="checkbox"/>	<input type="checkbox"/>		
disoriented	<input type="checkbox"/>	<input type="checkbox"/>		

- ◆ Loss of consciousness?  Yes  No  Victim not sure Unexplained Injury? Describe \_\_\_\_\_
- ◆ Any change or loss of hearing during/after strangulation/suffocation?  Yes  No Describe \_\_\_\_\_
- ◆ Any change or loss of vision during/after strangulation/suffocation?  Yes  No Describe \_\_\_\_\_
- ◆ How did your body/head feel during/after strangulation/suffocation? Describe \_\_\_\_\_
- ◆ Did the victim...  Urinate  Defecate  Feel the urge to do one or both? \_\_\_\_\_

FACE	EYES AND EYELIDS	NOSE	EARS
<input type="checkbox"/> red or flushed	<input type="checkbox"/> petechiae to r eye	<input type="checkbox"/> petechiae	<input type="checkbox"/> petechiae on ear(s)
<input type="checkbox"/> petechiae	<input type="checkbox"/> petechiae to l eye	<input type="checkbox"/> scratch(es) or abrasion(s)	<input type="checkbox"/> bleeding from ear(s)
<input type="checkbox"/> scratch(es) or abrasion(s)	<input type="checkbox"/> petechiae to r eyelid	<input type="checkbox"/> swelling	<input type="checkbox"/> bruising, discoloration, or petechiae behind ear(s)
<input type="checkbox"/> sweating	<input type="checkbox"/> petechiae to r eyelid	<input type="checkbox"/> other: (explain below)	<input type="checkbox"/> swelling
<input type="checkbox"/> bruising	<input type="checkbox"/> blood in eyeball(s)		<input type="checkbox"/> other: (explain below)
<input type="checkbox"/> other: (explain below)	<input type="checkbox"/> other: (explain below)		

Explain other: \_\_\_\_\_



MOUTH	UNDER CHIN	CHEST	SHOULDERS
<input type="checkbox"/> bruise(s) <input type="checkbox"/> swollen tongue <input type="checkbox"/> swollen lip(s) <input type="checkbox"/> scratch(es)/abrasion(s) <input type="checkbox"/> other: (explain below)	<input type="checkbox"/> redness <input type="checkbox"/> scratch(es)/abrasion(s) <input type="checkbox"/> laceration(s) <input type="checkbox"/> bruise(s) <input type="checkbox"/> fingernail impression(s) <input type="checkbox"/> other: (explain below)	<input type="checkbox"/> redness <input type="checkbox"/> scratch(es)/abrasion(s) <input type="checkbox"/> laceration(s) <input type="checkbox"/> bruise(s) <input type="checkbox"/> other: (explain below)	<input type="checkbox"/> redness <input type="checkbox"/> scratch(es)/abrasion(s) <input type="checkbox"/> laceration(s) <input type="checkbox"/> bruise(s) <input type="checkbox"/> other: (explain below)

Explain other: \_\_\_\_\_

NECK	HEAD
<input type="checkbox"/> redness <input type="checkbox"/> tenderness/pain <input type="checkbox"/> finger mark(s) <input type="checkbox"/> scratch(es)/abrasion(s) <input type="checkbox"/> fingernail impression(s) <input type="checkbox"/> bruise(s) <input type="checkbox"/> ligature mark(s) <input type="checkbox"/> petechiae <input type="checkbox"/> swelling <input type="checkbox"/> other: (explain below)	<input type="checkbox"/> petechiae on scalp or head <input type="checkbox"/> laceration(s) <input type="checkbox"/> scratch(es)/abrasion(s) <input type="checkbox"/> hair pulled <input type="checkbox"/> bump(s) <input type="checkbox"/> other: (explain below)

Explain other: \_\_\_\_\_

\*\*\*PLEASE TAKE PHOTOGRAPHS\*\*\*

Diagram all injuries on the Victim



Describe any other injuries or symptoms: \_\_\_\_\_

### OFFICER CHECKLIST

- If strangled/suffocated with object(s), photograph object(s) and collect for evidence.
- Document where the object(s) was/were found in the Offense Report.
- Determine if jewelry was worn by either party (ring(s), necklace(s), watch(es), etc.). Photograph / look for patterns and photograph.
- If defecation or urination in clothes, photograph clothing for evidence.
- If Victim vomited, take a photo of vomit for evidence.
- EMS called to evaluate victim for possible injury.

\_\_\_\_\_  
Reporting Officer

\_\_\_\_\_  
Date

\_\_\_\_\_  
Supervisor Approval

\_\_\_\_\_  
Date



# **City of Teague Police Department**

## **Job Descriptions**

## **Sworn Personnel**

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION

### POLICE OFFICER CLASSIFICATION

#### POSITION STATEMENT

A Teague Police Department Police Officer is called upon to perform a variety of tasks, both enforcement and non-enforcement related. This job description outlines those tasks (functions) and divides them into two categories, essential and marginal.

The essential functions are those tasks that a person must be able to perform, with or without reasonable accommodation, to obtain and maintain employment as a police officer for the City of Teague Police Department.

The marginal functions are those tasks that a police officer might be called upon to perform and should be able to perform with or without reasonable accommodation.

Duty assignment may be to any patrol shift or to any of the specialized function directed by the Chief of Police.

#### ENTRY LEVEL REQUIREMENTS

To be eligible for consideration for employment as a police officer for the City of Teague, a person must:

- Be a citizen of the United States,
- Be twenty-one years of age,
- Possess a high school diploma or G.E.D.,
- Possess a valid Texas driver's license,
- Possess a license or be eligible for licensing as a peace officer by the Texas Commission on Law Enforcement Officers Standards and Education, and
- Possess the abilities necessary to perform the essential functions of a police officer job as outlined in the job description.

#### WORK ENVIRONMENT

The working environment, for the most part, consists of working in an air-conditioned building with frequent and disruptive noise, or working outdoors or in an air-condition vehicle, frequently subject to intense or inadequate lighting, disruptive and extreme noise, extreme temperatures, dust/dirt, and constant exposure to various weather conditions, hazards, and accidents.

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION POLICE OFFICER

### CLASSIFICATION – CONTINUED

#### SUPERVISION RECEIVED AND EXERCISED

A police officer shall receive supervision from a Sergeant and/or the Chief of Police and additional supervision from higher level supervisory or management personnel within the city.

A police officer shall exercise supervision over other police officers at any assigned scene until properly relieved by supervisory or specialized personnel. In addition, a police officer assigned as a Field Training Officer shall exercise supervision over any assigned probationary officer.

---

ABILITIES REQUIRED – The following are the abilities required to perform the essential functions of the police officer job:

#### ORAL COMPREHENSION

The ability to understand words and sentences spoken in English.

#### WRITTEN COMPREHENSION

The ability to read and understand words, sentences and paragraphs written in English.

#### ORAL EXPRESSION

The ability to use English words and sentences in speaking so others will understand. Oral Expression includes the ability to communicate information and the meaning of ideas to other people. This ability involves knowledge of the meanings and distinctions among words and the way words should be put together to communicate the intended meaning of a message.

#### WRITTEN EXPRESSION

The ability to use English words and sentences in writing so others will understand. Written Expression includes the ability to communicate information and ideas in writing. This ability involves knowledge of the meanings and distinctions among words, strong working knowledge of grammar, and the ability to organize sentences and paragraphs.

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION POLICE OFFICER

### CLASSIFICATION – CONTINUED

#### MEMORIZATION

The ability to remember information, such as words, numbers, pictures and procedures. Pieces of information can be remembered by themselves or with other pieces of information. It emphasizes what cognitive psychologists call episodic memory which is the memory for specific events. This can be distinguished from semantic memory which refers to the general knowledge base.

#### PROBLEM SENSIVITY

The ability to tell when something is wrong or likely to go wrong. It includes being able to identify the whole problem as well as the elements of the problem.

#### NUMBER FACILITY

This ability involves the degree to which adding, subtracting, multiplying, or dividing can be done quickly and correctly. These procedures can be steps in other operations like finding percents or taking square roots.

#### DEDUCTIVE REASONING

The ability to apply general rules to specific problems to come up with logical answers. It involves deciding if an answer makes sense.

#### INDUCTIVE REASONING

The ability to combine separate pieces of information, or specific answers to problems, to form general rules or conclusions. This involves the ability to think of possible reasons why things go together. It also includes coming up with a logical explanation for a series of events which seem unrelated.

#### INFORMATION ODERING

The ability to correctly follow a rule or set of rules to arrange things or actions in a certain order. The rule or set of rules to be used must already be given. The things or actions to be put in order can include numbers, letters, words, pictures, procedures, sentences, and mathematical or logical operations.

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION POLICE OFFICER

### CLASSIFICATION – CONTINUED

#### SPEED OF CLOSURE

The ability to quickly make sense of information which initially seems to be without meaning or organization. It involves the degree to which different pieces of information can be combined and organized into one meaningful pattern quickly. The material may be visual or auditory.

#### FLEXIBILITY OF CLOSURE

The ability to identify or detect a known pattern (a figure, word or object) which is hidden in other material. The task is to pick out the pattern you are looking for from the background material.

#### SPATIAL ORIENTATION

The ability to tell where you are in relation to the location of some object or to tell where the object is in relation to you. It involves maintaining directional orientation as in one's bearings with respect to the points of a compass. This ability allows one to keep orientation in a vehicle as it changes location and direction. It helps one from getting disoriented or lost as one moves in a new environment.

#### VISUALIZATION

The ability to imagine how something will look when it is moved around or when its parts are moved or rearranged. It requires the forming of mental images of what patterns or objects would look like after certain changes such as unfolding or rotation. One has to predict what an object, set of objects or pattern would look like after the changes were carried out.

#### PERCEPTUAL SPEED

This ability involves the degree to which one can compare letters, numbers, objects, pictures or patterns, both quickly and accurately. The things to be compared may be presented at the same time or one after the other. This ability also includes comparing a presented object with a remembered one.

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION POLICE OFFICER

### CLASSIFICATION – CONTINUED

#### SELECTIVE ATTENTION

The ability to concentrate on a task without getting distracted. When distraction is present, it is not part of the task being done. This ability also involves concentrating while performing a boring task.

#### TIME SHARING

The ability to shift back and forth between two or more sources of information. The information can be in the form of speech, signals, sounds, touch or other sources.

#### RESPONSE ORIENTATION

The ability to choose between two or more movements quickly and accurately when two or more different signals (light, sounds, pictures, etc.) are given. The ability is concerned with the speed with which the right response can be started with the hand, foot or other parts of the body.

#### ARM-HAND STEADINESS

The ability to keep the hand and arm steady. It includes steadiness while making an arm movement as well as while holding the arm and hand in one position. The ability does not involve speed or strength.

#### MANUAL DEXTERITY

The ability to make skillful, coordinated movements on one hand, a hand together with its arm, or two hands to grasp, place, move or assemble objects like hand tools or blocks. This ability involves the degree to which these arm-hand movements can be carried out quickly. It does not involve moving machine or equipment control or levers.

#### STATIC STRENGTH

The ability to use continuous muscle force to lift, push, pull or carry objects. This ability can involve the hand, arm, back, shoulder or leg. It is the maximum force that one can exert for a brief period of time.

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION POLICE OFFICER

### CLASSIFICATION – CONTINUED

#### EXPLOSIVE STRENGTH

The ability to use short bursts of muscle force to propel one's self, as in jumping or sprinting, or to throw objects. It requires gathering energy for bursts of muscular effort.

#### DYNAMIC STRENGTH

The ability to support, hold up or move the body's own weight with the arms, repeatedly or continuously over time. The ability involves the degree to which the arm-shoulder muscles do not "give out" or fatigue when exerted in such repeated or continued movement.

#### TRUNK STRENGTH

This ability involves the degree to which one's stomach and lower back muscles can support part of the body or the position of the legs, repeatedly or continuously over time. The ability involves the degree to which these trunk muscles do not "give out" or fatigue when they are put under such repeated or continuous strain.

#### EXTENT FLEXIBILITY

The ability to bend, stretch, twist or reach out body, arms and/or legs.

#### DYNAMIC FLEXIBILITY

The ability to bend, stretch, twist or reach out with the body, arms and/or legs both quickly and repeatedly.

#### GROSS BODY EQUILIBRIUM

The ability to keep or regain one's body balance or to stay upright when in an unstable position. This does not include balancing objects.



# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION POLICE OFFICER

### CLASSIFICATION – CONTINUED

#### STAMINA

The ability to exert one's self physically over a period of time without getting winded or out of breath.

#### SOCIAL SENSIVITY

The skill of acting suitably in a social situation, regardless of the exact nature of the social contact. It involves adjusting your behavior to fit the social occasion. It depends on figuring out how other people feel.

#### ORAL FACT FINDING

The ability to uncover the important and relevant information about a problem through conversation, questioning or discussion.

#### RESISTANCE TO PREMATURE JUDGEMENT

The ability to withhold final decision until the important facts have been collected and evaluated.

#### PERSISTENCE

The ability to keep on trying to persuade others despite such factors as fatigue, distractions, boredom and resistance.

#### BEHAVIOR FLEXIBILITY

The ability to adapt one's behavior to changing circumstances when motivated to reach a goal.

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## ESSENTIAL FUNCTIONS OF POLICE OFFICER JOB CLASSIFICATION

The following are functions of the police officer job which a person must be able to properly perform to obtain and maintain employment as a Teague Police Department Police Officer:

1. Attend work regularly in accordance with agency leave policies,
2. Inspect vehicles for weapons or contraband at the start of the work shift and after each transport of prisoners or other persons,
3. Check the condition of the assigned vehicle and other equipment,
4. Identifies and requests needed repairs to vehicle and other equipment,
5. Communicates using the police radio,
6. Safely operates vehicles and emergency equipment in emergency situations,
7. Informs telecommunications, via radio or other means, of changes at any police scene,
8. Safely operates vehicles under extreme weather conditions and/or unusual road conditions,
9. Patrols and/or checks assigned areas to deter crime and be readily available in case of serious incidents,
10. Deals with mentally or emotionally disturbed persons,
11. Uses street guide/maps to become familiar with area,
12. Distinguishes legal from illegal activities,
13. Responds to calls for police assistance from citizens,
14. Responds to crimes in progress,
15. Investigates suspicious circumstances,
16. Identifies potentially hazardous situations and takes corrective actions,
17. Arrests and/or issues citations to traffic law violators,
18. Mediates domestic and family disputes and takes action according to departmental policies and family violence statutes,
19. Control hostile groups,
20. Uses restraints to subdue resisting persons according to departmental policies and statutes,

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## ESSENTIAL FUNCTIONS OF POLICE OFFICER JOB CLASSIFICATION

21. Conducts frisks and pat-down searches in accordance with departmental policies and within the framework of Terry v Ohio,
22. Makes arrests and uses force in accordance with departmental policies and statutes,
23. Conducts searches of arrested persons,
24. Handcuffs or otherwise restrains arrested persons,
25. Restrains violent or disorderly prisoners,
26. Safely and accurately discharges firearms when necessary,
27. Applies first aid in serious situations,
28. Requests emergency assistance at the scene of an accident or other emergency,
29. Takes precautions to prevent additional accidents at any police scene,
30. Administer or assists with cardio-pulmonary resuscitation,
31. Removes hazards from roadways,
32. Reports hazardous roadway conditions and defective traffic control devices,
33. Evacuates areas endangered by explosive or toxic substances,
34. Makes lawful arrests without warrants,
35. Makes lawful arrests with warrants,
36. Completes prisoner booking process in accordance with departmental policies,
37. Guards arrested persons outside secured detention facilities,
38. Searches persons, premises, autos, or property with consent or incident to arrest,
39. Searches persons, premises, autos, or property authorized by warrant,
40. Searches persons, premises, autos or property based on probable cause,
41. Conducts preliminary investigations on criminal offenses,
42. Conducts follow-up investigations as directed by supervisory personnel,
43. Prepares complete and understandable reports on criminal offenses and other incidents,
44. Apprehends and processes juvenile offenders,

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## ESSENTIAL FUNCTIONS OF POLICE OFFICER JOB CLASSIFICATION

45. Participates in firearms training,
46. Maintains clean and functional service weapons and equipment,
47. Prepares for and testifies in courts,
48. Attends and satisfactorily completes required in-service training,
49. Advises property owners or inhabitants of potentially dangerous conditions,
50. Provides intelligence information on known or suspected offenders to appropriate agency divisions or other agencies,
51. Conducts surveillance of individuals or groups to prevent or suppress criminal activity,
52. Assists emergency medical personnel with sick or injured persons,
53. Safely assists hazardous material team at scene of toxic spill,
54. Assists fire & Emergency Medical personnel at scene of fires or medical emergencies,
55. Distinguishes between hazardous and non-hazardous situations, and
56. Reads, understands and complies with all security and safety regulations.

## MARGINAL FUNCTIONS

The Teague Police Department Police Officer is assigned to single officer units; therefore, all functions are essential and there are no marginal functions.

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION

### SERGEANT CLASSIFICATION

#### POSITION STATEMENT

A Teague Police Department Sergeant must possess all the abilities outlined in the Teague Police Department Police Officer Classification job description and be able to perform all the essential functions outlined in that job description as well as the essential functions of the Sergeant Classification.

Duty assignment as a Teague Police Department Sergeant may be to a patrol supervisory assignment, criminal investigations or community resource coordinator. Assignment to a specific sergeant position is at the discretion of the Chief of Police and any sergeant may be reassigned to any sergeant position as deemed appropriate by the Chief of Police.

#### ENTRY LEVEL REQUIREMENTS

- Licensed as a Texas Peace Officer,
- Three years experience as a police officer,
- Above average oral and written communications skills, and
- Completion of T.C.O.L.E. First Line Supervisor's Course within twelve months after promotion to Sergeant.

#### WORK ENVIRONMENT

The working environment generally consists of working in an air-conditioned building with frequent interruptions and contact with irate and/or irrational persons, or working outdoors in an air-conditioned vehicle but frequently exposed to intense or inadequate lighting, disruptive and extreme noise, extreme temperatures, dust/dirt, and constant exposure to hazards and accidents.

Working hours might consist of any patrol shift, day time, weekend duty, holidays, on-call status and special events.

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION

### SERGEANT CLASSIFICATION – CONTINUED

#### SUPERVISION RECEIVED AND EXERCISED

A Teague Police Department Sergeant shall receive direct supervision from the Chief of Police and additional supervision from higher level police supervisory and management personnel within the city.

A sergeant shall supervise police officers as directed by the Chief of Police and shall supervise all personnel at a crime scene or incident until properly relieved by the Chief of Police or specialized personnel as outlined in departmental policies.

#### ABILITIES REQUIRED FOR SERGEANT CLASSIFICATION

A Teague Police Department Sergeant shall possess all the abilities required in the Police Officer Classification as well as above average oral and written communications skills.

#### ESSENTIAL FUNCTIONS SERGEANT CLASSIFICATION

The essential functions of the Sergeant Classification are divided into three assignment sections. A Teague Police Department Sergeant must be able to properly perform all the essential functions required of any assignment to patrol supervision, criminal investigations or community resources coordination.

#### ESSENTIAL FUNCTIONS PATROL ASSIGNMENT

1. Conduct shift briefings at beginning of shift,
2. Assign officers to special patrol duties as needed,
3. Conduct in-service training as directed by the Chief of Police,
4. Observe and evaluate police officer job performance,
5. Insure all personnel comply with laws and regulations,
6. Insure police officers comply with departmental policies,
7. Maintain officer time records in absence of the Chief of Police,
8. Approve/disapprove officer time off in absence of the Chief of Police,

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

9. Maintain shift schedule to insure sufficient coverage,
10. Supervise and assist officers at crime and incident scenes,
11. Inspect officer's vehicles and equipment,
12. Check officer's paperwork for completeness and accuracy,
13. Coordinate police activities with other agencies,
14. Coordinate activities with other departmental divisions,
15. Receive and process citizen complaints against any department member,
16. Compile and maintain statistical records as directed by the Chief of Police,
17. Keep the Chief of Police informed of all aspects of shift activity,
18. Call additional or specialized personnel to scene as needed,
19. Stay informed of all shift activity,
20. Attend supervisory meetings as scheduled,
21. Delegate authority and responsibility as directed by departmental policies and procedures, and
22. Good working knowledge of computer programs and Microsoft applications.

## MARGINAL FUNCTIONS

The Teague Police Department Sergeant position is assigned to single officer units; therefore, all functions are essential and there are no marginal functions.

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## CHIEF OF POLICE POSITION STATEMENT

The Chief of Police is under the administrative direction of the City Administrator, by direction of the Mayor and City Council. The Chief of Police is responsible for the effective management of the Police Department, Animal Control Services, Code Enforcement Services, and Fire Marshall's Office. The Chief of Police oversees all sub-departments within the police department to ensure that all City and Departmental Policies and Procedures are followed. The Chief of Police reviews and approves all department policies and procedures and assists in the creation of each department's yearly budget. All expenditures from each department must be approved by the Chief of Police.

The Chief of Police is responsible for planning, organizing, staffing, directing and controlling the police services for the City of Teague. The Chief of Police directs departmental managerial and operational staff towards achieving established goals and objectives. Work is performed with considerable discretion and latitude in interpreting and applying policies, rules and regulations.

### Qualifications

1. Must be a T.C.O.L.E. licensed Texas Peace Officer with an Advanced Peace Officer Certification, Master Peace Officer Certification preferred, and;
2. Possess a Bachelor's Degree from an accredited institution and three (3) years full time law enforcement experience with a municipal law enforcement agency, or possess an Associate Degree or sixty (60) credit hours from an accredited college or university institution and Five (5) years full time law enforcement experience with a municipal law enforcement agency, or Seven (7) years full time law enforcement experience with a municipal law enforcement agency, without any college credits, and;
3. Possess a valid Texas Operators License, and;
4. Possess the abilities to perform the essential functions of a Teague Police Officer as outlined in the Teague Police Officer Job Description,
5. Must have at least two years of experience in a senior level law enforcement capacity, E.g., rank of Lieutenant or higher within a law enforcement department, and;
6. Any other qualifications that the Board of Alderman may require.



# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION

### CHIEF OF POLICE CLASSIFICATION -

#### CONTINUED

#### Essential Job Functions

1. Performs and / or oversees departmental planning; develops the broad outline of the work to be done; establishes methods for accomplishing departmental objectives; ensures that departmental goals and objectives are consistent and compatible with goals and objectives set by the City of Teague,
2. Organizes the department to meet established goals and objectives; establishes formal lines of authority; establishes and maintains work groups to meet defined objectives,
3. Oversees the function of departmental staffing; identifies and documents departmental staffing needs; develops request and or proposals for additional staff,
4. Maintains continuous liaison with other department heads, city staff, and various outside agencies,
5. Oversees and administrates the department's budget; establishes controls and manages expenditures,
6. Interacts with the community on behalf of the department and the City; prepares and delivers speeches, lectures and presentations; represents the department and the City before various city and county boards, commissions and committees; responds to public inquiries and resolves complaints, and
7. Effectively supervises and recommends the hiring, discharge, evaluation assignment, discipline and adjustment of grievances of subordinate employees.

(NOTE: The duties listed above are intended as illustrations of the various types of work performed by the Chief of Police and are not limited to these duties. Other duties may be assigned as deemed necessary by the Mayor and City Council)

# TEAGUE POLICE DEPARTMENT JOB CLASSIFICATION

## JOB DESCRIPTION

### CHIEF OF POLICE CLASSIFICATION -

#### CONTINUED

#### Knowledge, Abilities and Skills

1. Principles, practices, and techniques of modern law enforcement,
2. Community geography and demographics,
3. Principles and practices of organization, management, budget development and personnel administration,
4. Federal, state, and local laws and ordinances that affect or are enforced by the police department,
5. Plan, evaluate, assign and coordinate activities performed by the police department,
6. Motivate, manage and supervise employees with varying levels of education and work experience,
7. Establish and maintain effective working relationships with City Administration, other city departments, public agencies, the news media and the general public,
8. Speak effectively and comfortably to large groups of people,
9. React calmly and quickly in emergency situations, and
10. Analyze complex managerial and administrative problems, formulate solutions and take independent unilateral action.



TEAGUE POLICE DEPARTMENT

315 MAIN STREET

TEAGUE, TEXAS 75860

### ***Citizen Complaint Process***

The Department will hear all complaints against its members, which have been initiated by any person that is found to have standing for such a complaint.

Complaints may be reported by phone, mail, internet, or in person. All complaints will be addressed. Following the first report of your complaint, you will be asked to provide a written statement and following that, the complaint will be investigated. All investigations of citizen complaints will be conducted in a timely matter. Depending on the nature of the complaint, some will take longer than others to investigate. Upon conclusion of the investigation you will be notified of the disposition of your complaint.

The Complaint process is a tool used to evaluate citizen concerns with regards to the performance and actions of our personnel and the agency itself. The process is not used to determine guilt or innocence or to debate the outcome of any legal proceeding; the appropriate court of venue will handle these legal proceedings.

Types of Citizen Complaints:

Generally there are two types of citizen complaints: those regarding a particular police service and those involving police personnel.

#### ***Police Service Complaints***

Are those types of complaints made regarding any service performed by the Police Department, and not specifically directed at an employee.

#### ***Police Personnel Complaints***

Are those types of complaints regarding the performance of duties, or behavior of Departmental personnel, which include, but of course are not limited to, violations of Federal, State and Local laws, and other rules established through Departmental policies and procedures.

These types of complaints are generally subdivided into two categories: complaints handled by the immediate supervisor and complaints handled by the Office of Internal Affairs: Examples of complaints handled by the immediate supervisor would be "Rudeness" or "minor driving violations" etc. Examples of complaints handled by the Office of Internal Affairs would be, violation of Federal, State or Local laws, Excessive Force, etc.



TEAGUE POLICE DEPARTMENT  
315 MAIN STREET  
TEAGUE, TEXAS 75860

**What is the law regarding making a complaint on a police officer?**

Texas Government Code § 614.022. Complaint to be in Writing and Signed by Complainant

To be considered by the head of a state agency or by the head of a fire or police department, the complaint must be:

- (1) in writing; and
- (2) signed by the person making the complaint.

Texas Government Code § 614.023. Copy of Complaint to be Given to Officer or Employee

- (a) A copy of a signed complaint against a law enforcement officer, fire fighter, or police officer shall be given to the officer or employee within a reasonable time after the complaint is filed.
- (b) Disciplinary action may not be taken against the officer or employee unless a copy of the signed complaint is given to the officer or employee.

Texas Penal Code § 37.02. Perjury

- (a) A person commits an offense if, with intent to deceive and with knowledge of the statement's meaning:
  - (1) he makes a false statement under oath or swears to the truth of a false statement previously made and the statement is required or authorized by law to be made under oath; or
  - (2) he makes a false unsworn declaration under Chapter 132, Civil Practice and Remedies Code.
- (b) An offense under this section is a Class A misdemeanor.

***Instructions***

This form should be completed with as much details as possible and signed in front of a Police Notary.  
The completed form should be brought to the Teague Police Department at 315 Main Street.



TEAGUE POLICE DEPARTMENT

315 MAIN STREET

TEAGUE, TEXAS 75860

PERSON MAKING COMPLAINT

Last			First		Middle
Sex	Race	Date of Birth	Drivers License#	State of DL	
Home phone			Work phone		Cell Phone
Email					
Address/City/State/Zip Code					

INCIDENT IN QUESTION

Date of Incident	Time of Incident	Location of Incident

Name or description of Officer(s) Involved



TEAGUE POLICE DEPARTMENT

315 MAIN STREET

TEAGUE, TEXAS 75860

Name of Person directly affected by this Incident:

Last		First			Middle
Sex	Race	Date of Birth	Drivers License#	State of DL	
Home phone		Work phone		Cell Phone	
Email					
Address/City/State/Zip Code					

How was this person affected (Arrested, Citation, Jailed, Injured, Questioned and Released, Other)
What is your standing to make this complaint (Person affected, Concerned Citizen, Parent)

What did the Officer do that prompted you to make this complaint; (Violated a Law (Be Specific), Made Illegal Stop, Conducted Illegal Search, Used Profanity, Used Unnecessary Force, Was Rude in dealing with the Public)



TEAGUE POLICE DEPARTMENT  
315 MAIN STREET  
TEAGUE, TEXAS 75860

Please write a brief narrative of your complaint (If additional space is needed attach a separate page to this form)

A large, empty rectangular box with a black border, intended for writing a narrative of a complaint.



TEAGUE POLICE DEPARTMENT  
 315 MAIN STREET  
 TEAGUE, TEXAS 75860

WITNESSES THAT HAVE DIRECT KNOWLEDGE OF THIS INCIDENT (If there are additional witnesses please attach a separate page to this form)

Last			First		Middle
Sex	Race	Date of Birth	Drivers License#	State of DL	
Home phone			Work phone		Cell Phone
Email					
Address/City/State/Zip Code					

Last			First		Middle
Sex	Race	Date of Birth	Drivers License#	State of DL	
Home phone			Work phone		Cell Phone
Email					
Address/City/State/Zip Code					

Last			First		Middle
Sex	Race	Date of Birth	Drivers License#	State of DL	
Home phone			Work phone		Cell Phone
Email					
Address/City/State/Zip Code					





TEAGUE POLICE DEPARTMENT

315 MAIN STREET

TEAGUE, TEXAS 75860

Person Making Complaint

Last	First	Middle

**PRINT NOW. Do not sign until delivered to Police Notary. Please call to set appointment.**

ANY FALSE STATEMENTS MADE MAY BE SUBJECT TO PROSECUTION UNDER PERJURY, FALSE REPORT OR CIVIL STATUTES. UNDER PENALTY OF PERJURY THE UNDERSIGNED SWEARS THAT THE FACTS CONTAINED ON THIS COMPLAINT FORM, AND ALL ATTACHMENTS OF THIS DOCUMENT, ARE WITHIN THEIR PERSONAL KNOWLEDGE AND ARE TRUE AND CORRECT.

\_\_\_\_\_  
Signature of Complainant

On the \_\_\_\_\_ day of \_\_\_\_\_ 20 \_\_\_\_

personally appeared \_\_\_\_\_ who on their oath stated the above facts were true and correct.

\_\_\_\_\_  
(Seal)

Notary

\_\_\_\_\_  
Signature of City Official Receiving Complaint

\_\_\_\_\_  
Date Received

**TEAGUE POLICE DEPARTMENT**

**Use of Force Supplement**

**Use of Force:**  
Date: \_\_\_\_\_ Time: \_\_\_\_\_ Day of Week: \_\_\_\_\_ Shift: \_\_\_\_\_ Area: \_\_\_\_\_ Arr/Off.#: \_\_\_\_\_  
Primary Officer Using Force: \_\_\_\_\_ # \_\_\_\_\_ Time on Dept: \_\_\_\_\_ Years \_\_\_\_\_ Mos. \_\_\_\_\_  
Location: \_\_\_\_\_ Call Type: \_\_\_\_\_ Type Premises: \_\_\_\_\_  
Subject Name: \_\_\_\_\_ Race: \_\_\_\_\_ Sex: \_\_\_\_\_ DOB: \_\_\_\_\_ Age: \_\_\_\_\_  
Address: \_\_\_\_\_ Hgt: \_\_\_\_\_ Wgt: \_\_\_\_\_  
Subject Injured:  No  Yes: \_\_\_\_\_  
Transported to: \_\_\_\_\_  Amb.  Refused Treatment  
Officer Injury:  No  Yes: \_\_\_\_\_  
Transported to: \_\_\_\_\_  Amb.  Refused Treatment

**Reason for Use of Force:**  
 To Effect Arrest  To Defend Another Officer  To Prevent Offense  
 To Defend Self  To Defend Another Person  Restrain for Subject Safety  
 Other: \_\_\_\_\_

**Subject's Actions:**  
 Nonverbal cues indicating physical resistance  
 Verbal threats, non-compliance with officer direction  
 Dead weight, clinging to objects, preventing custody  
 Pulling, pushing, running away, to avoid control, not harming officer  
 Assault, grabbing, pushing, kicking, striking officer or another  
 Assault with intent and ability to cause death or SBI  
 Assault or threats with deadly weapon  
 Other: \_\_\_\_\_  
Number of Suspects Resisting: \_\_\_\_\_  
Appeared or Known Under the Influence  
 Alcohol  
 Drugs  
 Mental issues  
 Other: \_\_\_\_\_

**Officer Actions:** (Check all that apply, if more than one type of force used, number in order of use.)  
 Verbal Direction  Less Lethal Munitions (Bean bag, stinger, rubber)  
 Soft Weaponless Control (Muscling, joint locks, pressure points)  Pointed Taser (Laser)  
 Hard Weaponless Control (Hard strikes, leg strikes, shoulder pin)  Discharged Taser  
 OC Spray  Pointed Firearm  
 Asp/Baton  Discharged Firearm  
 Non-Lethal (Pepperball)  Other: \_\_\_\_\_

**Physical Control:**  
 Not Used  Pressure Points  Takedown  Hobble  
 Muscling (grip, push, pull)  Joint Lock  Handcuffing  Other: \_\_\_\_\_  
Effective:  Yes  No: \_\_\_\_\_

**OC Spray:**  
OC Spray:  Not Used  Attempted  Used Distance: \_\_\_\_\_ - \_\_\_\_\_ ft. Duration: 1: \_\_\_\_\_ 2: \_\_\_\_\_ 3: \_\_\_\_\_  
Effective:  Yes  No: \_\_\_\_\_

**ASP / Baton:**  
ASP / Baton:  Not Used  Used Number of Strikes: \_\_\_\_\_ Location: \_\_\_\_\_  
Effective:  Yes  No: \_\_\_\_\_

**Non Lethal / Less Lethal Munitions:** (insert number of rounds fired / hits)  
Non/Less lethal Munitions:  Not Used  Used Bean Bag: \_\_\_\_\_ Stinger: \_\_\_\_\_ Rubber: \_\_\_\_\_ Pepperball: \_\_\_\_\_  
Location of Hits: \_\_\_\_\_  
Effective:  Yes  No: \_\_\_\_\_





# Teague Police Department

315 Main Street  
 Teague, Texas 75860  
 Phone: (254) 739-2553 Fax: (254) 739-3213  
 DeWayne Philpott, Chief of Police

## VEHICLE MONTHLY CHECK SHEET

<b>VEHICLE</b>		<b>DATE SUBMITTED</b>		<b>OFFICER SUBMITTING</b>	
<b>CURRENT MILEAGE</b>		<b>IS VEHICLE DOWN</b>		<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> N/A	

### MECHANICAL

<input type="checkbox"/>	NEEDS OIL CHANGE
<input type="checkbox"/>	NEEDS TIRES ROTATED
<input type="checkbox"/>	HEADLIGHT/BRAKELIGHT/TURN SIGNAL LIGHT OUT
<input type="checkbox"/>	LICENSE PLATE LIGHT OUT
<input type="checkbox"/>	NEEDS BRAKES CHECKED/REPLACED
<input type="checkbox"/>	CHECK ALIGNMENT
<input type="checkbox"/>	NEEDS WINDSHIELD WIPER BLADES
<input type="checkbox"/>	NEEDS NEW TIRES
<input type="checkbox"/>	CHECK FRONT END
<input type="checkbox"/>	CHECK REAR END
<input type="checkbox"/>	HVAC NOT WORKING
<input type="checkbox"/>	OTHER (DETAIL IN NOTES)

### EMERGENCY/POLICE EQUIPMENT

<input type="checkbox"/>	IN CAR CAMERA MALFUNCTION
<input type="checkbox"/>	RADAR PROBLEM
<input type="checkbox"/>	LIGHT/SIREN CONTROLLER PROBLEM
<input type="checkbox"/>	EMERGENCY LIGHT OUT
<input type="checkbox"/>	EQUIPMENT MISSING (DIGITAL CAMERA, POLICE TAPE, ETC)
<input type="checkbox"/>	OTHER (DETAIL IN NOTES)

### OTHER

<input type="checkbox"/>	OTHER (DETAIL IN NOTES)
--------------------------	-------------------------

### NOTES


04/05/2019

<b>DATE RECVD</b>		<b>DATE SENT</b>		<b>EXPECT COMPLT</b>		<b>DATE COMPLT</b>		<b>DATE ENTERED</b>	
<b>BY</b>		<b>BY</b>		<b>BY</b>		<b>BY</b>		<b>BY</b>	

# TEAGUE POLICE DEPARTMENT

## Vehicle Pursuit Supplement

**Pursuit:**  
Date: \_\_\_\_\_ Start Time: \_\_\_\_\_ End Time: \_\_\_\_\_ Day of Week: \_\_\_\_\_ Arr/Off#: \_\_\_\_\_  
Beginning Location: \_\_\_\_\_  
Ending Location: \_\_\_\_\_  
Reason for Pursuit: \_\_\_\_\_  
Initiating Officer: \_\_\_\_\_ # \_\_\_\_\_ Secondary Officer: \_\_\_\_\_ # \_\_\_\_\_  
Controlling Supervisor: \_\_\_\_\_ # \_\_\_\_\_

**Conditions:**

<b>Weather</b>	<b>Road</b>	<b>Visibility</b>	<b>Traffic</b>	<b>Pedestrian</b>
<input type="checkbox"/> Cold	<input type="checkbox"/> Dry	<input type="checkbox"/> Clear/Daylight	<input type="checkbox"/> Light	<input type="checkbox"/> Light
<input type="checkbox"/> Cool	<input type="checkbox"/> Rain/Wet	<input type="checkbox"/> Fog/Smoke	<input type="checkbox"/> Medium	<input type="checkbox"/> Medium
<input type="checkbox"/> Warm	<input type="checkbox"/> Ice/snow	<input type="checkbox"/> Dawn/Dusk	<input type="checkbox"/> Heavy	<input type="checkbox"/> Heavy
<input type="checkbox"/> Hot	_____	_____	_____	_____

**Route and Distance:**  
Route: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
Total Distance: \_\_\_\_\_ High Speed: \_\_\_\_\_ Total time: \_\_\_\_\_

**Tire Deflation Devices:**  
Tire Deflation Devices Used:  Used  Attempted  Not Attempted Effective:  Yes  No  
Reason: \_\_\_\_\_

**Termination of Pursuit:**  
Method of Termination

<input type="checkbox"/> Stopped Voluntarily	<input type="checkbox"/> Mechanical Failure	<input type="checkbox"/> Collision	<input type="checkbox"/> With Officer
<input type="checkbox"/> Terminated by Officer	<input type="checkbox"/> Terminated by Supervisor		<input type="checkbox"/> With Fixed Obj/Loss Control
<input type="checkbox"/> Other: _____			<input type="checkbox"/> With Citizen Vehicle

**Results of Pursuit:**  
Suspect:  Evaded  Arrested Charges: \_\_\_\_\_  
Property Damage:  None  Damage: \_\_\_\_\_  
Injury:  None  Injuries: \_\_\_\_\_

**Suspect:**  
Name: \_\_\_\_\_ DOB: \_\_\_\_\_ Age: \_\_\_\_\_ Injured:  Yes  No

\*\*\* Full Narrative of Pursuit in Arrest or Offense Report - Attach Copy to this Supplement \*\*\*

\*\*\*Officers should indicate any other significant events which occurred in the narrative\*\*\*

**Supervisor:**  
Total Units engaged Code 3: \_\_\_\_\_ Total Code 3 at any one time: \_\_\_\_\_  Video Reviewed  
Comments: \_\_\_\_\_  
\_\_\_\_\_  
Supervisor: \_\_\_\_\_ # \_\_\_\_\_  In Compliance with Policy  Further Investigation Needed

Reviewed: \_\_\_\_\_ In Compliance  Investigation Needed

**Patrol Sergeant**

Reviewed: \_\_\_\_\_ In Compliance  Investigation Needed

**Chief of Police**

**VOIDED CITATION MEMO**

Officer: \_\_\_\_\_ Voided Citation Number # \_\_\_\_\_

On \_\_\_\_\_  
(Date)

Brief narrative explaining the reason the citation was voided:

---

---

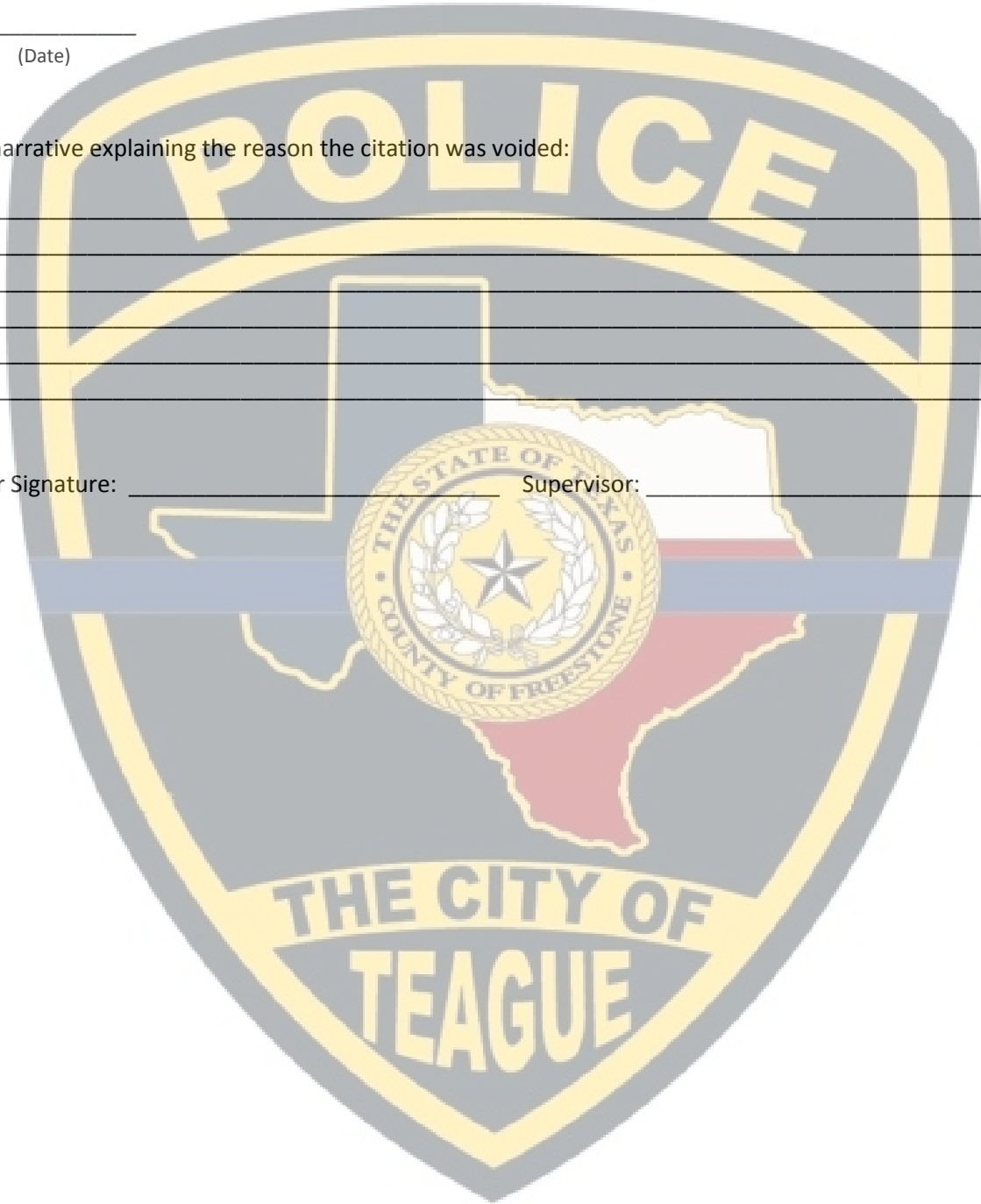
---

---

---

---

Officer Signature: \_\_\_\_\_ Supervisor: \_\_\_\_\_













# Teague Police Department

## Background Investigation Manual



*Date Adopted*

## ***CONDUCTING THE BACKGROUND INVESTIGATION***

### ***THIS MANUAL PROVIDES A STRUCTURED PROCEDURE TO HELP YOU ACQUIRE, ORGANIZE AND REPORT BACKGROUND INFORMATION ON YOUR POLICE OFFICER APPLICANTS***

A proper background investigation is an objective, fact-finding process that results in an accurate record of a candidate's past conduct and behavior. Your job, if you are a background investigator, is to investigate and report the pertinent aspects of the candidate's background, not evaluate those facts. Your investigation, therefore, should be descriptive, not evaluative.

Your objective is to provide sufficient information so the Police Chief or administrator making the employment decision can judge the significance of a candidate's past conduct in relation to the job requirements.

The background investigator's role can be distinguished from that of a criminal investigator in at least one important way. A criminal investigator is typically oriented toward negative information. Facts that might mitigate the significance of a crime or demonstrate the suspect's personal strengths and abilities are matters to be considered by the defendant's attorney or perhaps his/her probation officer, not the criminal investigator.

A background investigator, however, must consider both negative and positive information. While it is important to investigate all incidents in the background of candidates which may reflect unfavorably upon their ability to perform satisfactorily as police officers, it is equally important to include information on any mitigating circumstances surrounding an incident, which might explain or diminish its significance.

Finally, the rights of the candidate should be safeguarded throughout the process. One of those rights is the right to a fair, careful, and thorough evaluation of his/her candidacy. Another important right is the right of privacy. There is always the potential for conflict between the department's right to certain information concerning the candidate's background and the candidate's right to privacy. It is the investigator's responsibility to avoid unwarranted invasion of a candidate's privacy while, at the same time, developing the information necessary for a sound judgment as to the candidate's suitability for employment. This responsibility requires (1) that only job-related inquiries be made, and (2) that the information obtained be treated as strictly confidential.

### **THE PERSONAL HISTORY STATEMENT**

The basic document on which your background investigation should be based is the Personal History Statement completed by the applicant. The candidate should be provided with a copy of the Personal History Statement and given a reasonable

length of time to complete and return it. At the same time, candidates should be given a list of the documents which they will be required to provide.

These documents include:

- Copy of the applicant's Social Security card.
- Original certified copy of applicant's birth certificate. (No photocopy)
- Copy of applicant's valid Texas driver license or a copy of another State's driver license. Applicant must possess a valid Texas driver license prior to being offered employment.
- Copy of applicants High School diploma or GED certificate.
- Sealed original certified copy of applicant's college transcript. (No photocopy)
- Photocopy of applicant's college diploma.
- Copy of applicant's Peace Officer Certificate from applicant's police academy. (Peace Officer Applicants Only)
- Copy of applicant's Texas peace officer license and all training certificates awarded. (Peace Officer Applicants Only)
- Copy of applicant's DD-214 if applicable. Must possess an honorable discharge.
- Original certified copy of applicant's Naturalization papers, if applicable. (No photo copy)
- Copy of current proof of automobile liability insurance.

Where possible, the applicant should be told as early in the selection process as possible, which documents will be required for the background investigation. Also, the applicant should be fingerprinted, and requests for criminal records sent to the appropriate agencies as early as possible, including the FBI.

## **INVESTIGATIVE CONSIDERATIONS**

Throughout the investigation, the investigator should keep in mind the following:

### **1. Confidentiality**

- a. The information given by an applicant in the Personal History Statement, and information obtained by the investigator is private and confidential. At no time during the investigation or thereafter, should any portion of the investigation be revealed to persons other than those who are authorized to evaluate the results.
- b. As a general rule, the information gathered from third persons during the background investigation should not be revealed to the applicant. Only department officials authorized to evaluate the applicant should have access to this information. However, under various circumstances, the applicant may become aware of the contents of the investigation. For example, during the discrepancy interview some information may be disclosed when the applicant is questioned about

inconsistencies or contradictions between information given in the Personal History Statement and that obtained during the investigation. During the discrepancy interview, the investigator should avoid revealing the source of any information.

- c. Other situations in which an applicant may have access to background investigation information from third persons would include federal administrative action by the Equal Employment Opportunity Commission, and state and federal court actions. These administrative agencies and courts may have rules of procedure and evidence which would give the applicant access to information gained during the background investigation.
- d. Medical information: Information gathered during the medical examination is subject to the same confidentiality restrictions as the above information. Medical or mental health information should be referred to the examining physician. All of the information gathered is to be used solely to make a sound judgment as to the applicant's physical and mental ability to perform the job of a law enforcement officer, and no medical information can be collected until after a conditional offer of probationary employment has been made. Medical records must be kept in a separate, restricted access file, or a sealed envelope in the regular file folder, with access only on a need-to-know basis.

## **2. Demeanor of Investigating Officer**

The applicant and all other persons contacted during the course of the investigation may not have had prior personal contact with a law enforcement officer. It is important that they be left with a feeling that courtesy, integrity, and thoroughness are qualities of law enforcement officers in general, and of the law enforcement agency represented by the investigator.

## **3. Discontinuance of Investigation**

If, during the course of the investigation, information is obtained which will positively lead to rejection of the candidate, the investigator should consult with the appropriate superior officer to determine if the investigation should be discontinued.

## **4. Objectivity**

It is very important that the investigator maintain objectivity throughout the investigation. No personal biases should affect the quality and content of the investigation.

## **5. Evaluation of References**

The investigator should carefully evaluate all relatives, references, acquaintances, and other contact persons to determine their qualifications to speak on various aspects of the applicant's character. Consider: (1) the type of interaction the individual had with the applicant, (2) the duration and recency of that contact, and (3) any relevant education, training, experience, or specialized knowledge the individual may have.

## **BEGINNING THE INVESTIGATION**

To begin the background investigation, the investigator should carefully review the signed, completed Personal History Statement. It is the basic document of the investigation. It should be checked for inconsistencies, conflicting statements, or omissions. It should be checked against the initial application form, and should be checked against all verifying documents. The investigator should note any incomplete items, for discussion with the applicant.

Next, the investigator conducts a preliminary interview with the applicant, reviews the Personal History Statement for completeness and clarity, and discusses any questionable areas. Where the Personal History Statement reveals unusually favorable or unfavorable information, the investigator obtains further details from the applicant.

During the initial phases of the investigation, the investigator assembles the necessary documents to verify the applicant's birth date, fulfillment of the high school education requirement, military service, U. S. citizenship, and possession of a valid Texas driver's license. These documents should be secured from the applicant, copied, and returned to the applicant to ensure that they are not lost or misplaced.

To speed up the process, records that will take some time to obtain should be requested as soon as possible. For example, fingerprint cards should be sent immediately to the Department of Public Safety and to the F.B.I. A request for all previous law enforcement employment should be sent to TCLEOSE.

## **PREPARING A FOLDER OR A WORK SHEET**

The investigator catalogues the documents which are needed to verify compliance with all requirements, or which are needed to support other facts. The list should include the following:

### **1. Birth Date:**

- a. Any offered documentation to verify date of birth, to facilitate criminal history checks;

### **2. Required Education:**

- a. High school diploma, or
- b. General Educational Development (G.E.D.) certificate, or

- c. Other education and training that is claimed, such as college transcripts

### **3. Valid Texas driver's license**

The names, addresses and telephone numbers of persons to be contacted or personally interviewed are obtained, so that these people can be contacted in a logical sequence. To save time, appointments should be made in advance. The investigator's schedule should be kept flexible to enable him or her to follow leads developed during the investigation.

A separate list of persons or sources of information that require contact by mail is also made. For example, requests must be made by mail to the F.B.I., the Department of Public Safety, TCLEOSE, courts, and some out-of-town or out-of-state references. Subsequent sections in this manual provide more information on specific information sources which will require mailed inquiries.

### **SECURING NECESSARY FORMS AUTHORIZING RELEASE OF INFORMATION**

Before the investigation begins, the investigator has the applicant sign a form or forms authorizing the release of information. These forms should be completed and signed by the applicant in sufficient quantity to provide at least one for each school, financial and employment source identified in the Personal History Statement.

Special precautions should be taken when soliciting financial information. It is a good idea to require the investigator to present a copy of the release to each source interviewed or questioned, to verify that the investigation is for employment purposes.

For military records information, the applicant must sign the release authorization block of the "Request Pertaining to Military Records" If medical information from a private firm or physician is necessary, an appropriate authorization for release of medical records is needed. However, such information can only be sought after a Conditional Offer of Probationary Employment, and not before, or it would violate the Americans with Disabilities Act.

### **SENDING LETTERS OF INQUIRY AND REQUESTS FOR INFORMATION**

Personal interviews are preferable to mailed inquiries, since more information can be obtained, and the source of information evaluated. When interviews are impractical, sources of information should be contacted by mail. The investigator should determine what letters or requests for information forms must be mailed. Replies should be reviewed by the investigator as soon as they are received, and any questionable areas pursued before the investigation is terminated. People are more likely to comply with your requests if you enclose a self-addressed, stamped envelope.

### **INTERVIEWING**



Suggested interview questions on various topics are provided under the appropriate topic headings throughout this manual. The investigator should try to obtain specific facts to support any general statements given.

Take complete notes of all interviews, in order to ensure accuracy. Quoting or paraphrasing is preferred over subjective conclusions. Be sure to record the name, address, and telephone number of each person interviewed, as well as the date, time and location of the interview.

### **DISCREPANCY INTERVIEW**

Once the background investigation has been completed (or during the course of the investigation), if the investigator becomes aware of inconsistencies or contradictions between information supplied in the Personal History Statement and that obtained during the investigation, he/she should schedule a discrepancy interview with the applicant to resolve the questionable areas. The investigator should not reveal the source of any information obtained during the background investigation.

### **FINAL EVALUATION OF THE APPLICANT**

The background investigator is in the best position to evaluate the applicant's personal characteristics. From the facts gathered, the investigator writes a final report which summarizes all the facts gathered, including a final section which summarizes his/her evaluation of the applicant's qualifications with regard to the job dimensions. The investigator does not make the final hire/no-hire recommendations, but leaves that decision to the department head, which controls the total selection process.

### **NARRATIVE REPORT AND SUMMARY**

The written report should be complete, concise, and in narrative form. All documents and material necessary to verify compliance with departmental and TCLEOSE requirements should be submitted with the report to the Police Chief or the administrative officer designated to receive, review and evaluate it. Included with the report should be verifying documents, unused signed authorizations, returned forms and letters, the investigator's notes of interviews, and any other pertinent material. The report should be factual. For completeness, all information should be included. This will also facilitate a sound judgment of the applicant's qualifications. Persons interviewed should be either quoted verbatim or paraphrased.

A narrative report and summary will help the investigator to organize and write the final evaluation. Summaries should be included along with the narrative report, to form the basis for the investigator's evaluation. The following areas of inquiry are suggested for the narrative report. They follow the major sections on the Personal History Statement:

- A. Application Identification
- B. Residences

- C. Experience & Employment
- D. Military History
- E. Education
- F. Special Qualifications & Skills
- G. Legal
- H. Motor Vehicle Operation
- I. Relatives
- J. References & Acquaintances
- K. Financial





# Teague Police Department

315 Main Street

Teague, Texas 75860

Phone: (254) 739-2553 Fax: (254) 739-3213

DeWayne Philpott, Chief of Police

---

## ***SAMPLE NARRATIVE REPORT FOR A BACKGROUND INVESTIGATION***

To: Chief

From: Background Investigator

Subject: Background Investigation: Charles T. Candidate

### **PERSONAL**

The applicant Charles T. Candidate resides at 201 State Street, Dallas, Texas 75201. He can be contacted through his home phone, 225-1234, or work telephone, 228-4321. Mr. Candidate was born on July 10, 1952. His social security number is 002-26-8154. Mr. Candidate is 5'11" tall, weighs 160 pounds, has brown hair and blue eyes. He has no scars, tattoos or other distinguishing marks. All of the above facts have been confirmed, and verifying documents are attached.

### **RELATIVES, REFERENCES AND ACQUAINTANCES**

#### **Relatives**

All of the listed relatives with the exception of Mr. Candidate's older brother were contacted with no negative information. All stated that they felt Mr. Candidate would make a good peace officer in that he is willing to confront problems, is dependable, and has demonstrated that he is interested in people and has a high degree of interpersonal sensitivity. They also related that there was no question of Mr. Candidate's integrity.

Since Mr. Candidate's older brother, James Candidate, lives on the West Coast, he was not contacted.

#### **Prior Spouse**

Contact was made with Mr. Candidate's prior spouse, Lois Little. Mrs. Little related that the reason for the marriage dissolution was because of irreconcilable differences. She went on to state that, in her opinion, Mr. Candidate was immature, and that this has been demonstrated by the way he has "always squandered money." As an example, Mrs. Little stated that Mr. Candidate had

difficulty with paying bills on time and would waste what little money they had on fixing his motorcycle. This was the only derogatory information that Mrs. Little provided.

It should be noted that subsequent investigation revealed that Mr. Candidate was married for only six months and the marriage occurred when he was eighteen years of age.

Mr. Candidate's marriage dissolution prior to his current marriage has been verified and copies of the necessary documents are attached.

### **Offspring**

Mr. Candidate has no children.

### **Persons with Whom the Applicant has Resided**

Contact was made with Bill Smith, Mr. Candidate's roommate during college. Mr. Smith related that he was good friends with Mr. Candidate and that they still see each other occasionally. Mr. Smith stated that he is aware of Mr. Candidate's difficulties with finances, but stated that he never experienced any personal inconveniences because of Mr. Candidate. He stated that, to his knowledge, Mr. Candidate did pay his necessary bills and was always prompt to pay his half of the rent. Mr. Smith stated that, in his opinion, Mr. Candidate would make a good officer and that he is very interested in people and is willing to confront problems. An example of his willingness to confront problems is the fact that Mr. Candidate realized after a short period of time that his marriage was not beneficial to either himself or his prior spouse, and they amicably sought adissolution.

### **References and Acquaintances**

All the listed individuals were contacted. None had any negative information to convey.

Mr. Candidate's listed acquaintance, Tom Kaine, provided an additional name of Sara Smothers, 21 Avery Street Fort Worth, Texas 76201. Contact telephone 524-5614.

Ms. Smothers dated Mr. Candidate for a short period of time after Mr. Candidate's divorce. Ms. Smothers related that her relationship with Mr. Candidate was casual, but that he never exhibited any lack of dependability, had good interpersonal sensitivity, and she had no reason to believe that he could not handle his finances.

## **EDUCATION**

### **High School**

Mr. Candidate graduated from Concord High School in June, 1970, and this was confirmed by a copy of his high school diploma, which is attached.

Contact was made with Mr. Candidate's counselor, Mr. Fish, who stated that Mr. Candidate had always exhibited good learning ability. Although he never

made the honor roll, Mr. Fish believed that he could have, if he had asserted himself. Mr. Candidate has never been suspended or expelled from school.

### **Post-Secondary School**

Mr. Candidate attended the University of Texas at Austin for three years from 1971 through 1974. Mr. Candidate's listed advisor was contacted and he stated that he only knew Mr. Candidate briefly, and only discussed Mr. Candidate's educational future with him when he first came to the college in 1971. Mr. Larson, Mr. Candidate's advisor, stated that he knew of no reason why Mr. Candidate would not make a good law enforcement officer.

### **RESIDENCES**

#### **Neighbors and Landlords**

Mr. Candidate lived with his parents until he was first married. Mr. Candidate and his first wife lived in a large apartment complex at 322 Ocean Street, Arlington, Texas. A neighborhood check proved negative in locating anyone who remembered Mr. Candidate. Records were not maintained and thus no information was available on his reliability in paying the rent.

After his divorce, Mr. Candidate lived with a roommate, Mr. Smith, in an apartment complex at 2100 Howe Avenue, Addison, Texas. A neighborhood check proved negative in locating anyone who recalled Mr. Candidate or his roommate, Mr. Smith. A check with the manager revealed that they did maintain records back to 1971 and that the record revealed that Mr. Candidate and Mr. Smith paid their rent on time every month.

Neighbors where Mr. Candidate and his present wife now reside were contacted. Mr. and Mrs. Jones, who live on the west side of Mr. Candidate, stated that they thought Mr. Candidate and his wife "were a very nice couple." Mr. Jones stated that he thought Mr. Candidate would make a good peace officer and he had nothing derogatory to say about Mr. Candidate. All other neighbors confirmed this assessment.

### **EXPERIENCE AND EMPLOYMENT**

#### **Present and Past Employers and Supervisors**

During a check of Mr. Candidate's employment record, Mr. Knudsen, owner of Knudsen's Chevron Station, was contacted. Mr. Candidate was employed as a service station attendant at Knudsen's Service Station from 1968 through 1971, when he resigned to accept employment with Best Auto Parts while attending college. Mr. Knudsen stated that Mr. Candidate was one of the best employees he had ever had. Mr. Knudsen also stated that Mr. Candidate was dependable, punctual, got along well with fellow employees and was never any trouble. Mr. Knudsen did relate that on one occasion he had to return to the station late in the evening and found Mr. Candidate asleep; however, this was a single incident and was due to the fact that Mr. Candidate had stayed up all night the previous evening studying.

Mr. Candidate's present employer, Mr. Edward Best, related that Mr. Candidate is an excellent employee and he had no negative information to provide.

**Present and Past Co-workers:**

Mr. Candidate's past co-workers were available for interview. Mr. Dean Whittier related that Mr. Candidate was a good person to work with and that he had known Mr. Candidate for approximately two and a half years. Mr. Whittier had no negative information and said that he found Mr. Candidate to be very dependable, interested in people, and honest.

Mr. Candidate has never filed any claims for unemployment or workers' compensation. All time was accounted for in his background and he has no extended work absences.

Mr. Candidate has never been fired or asked to resign from employment. He has never been rejected for any other peace officer position.

**MILITARY**

Mr. Candidate has never served in the military.

**FINANCIAL**

In reviewing Mr. Candidate's financial statement, it was found that Mr. Candidate handles his finances well and apparently has not overextended himself. A check with the Concord Credit Bureau showed that Mr. Candidate had satisfactory credit and no delinquent payments.

Apparently, whatever difficulties Mr. Candidate had in the past due to financial reasons have been corrected.

Mr. Candidate has never filed bankruptcy, had any bills sent to a collection agency, had any purchased goods repossessed, had his wages attached, or been delinquent in paying taxes or rent payments.

**LEGAL**

A check with the Dallas, Austin, Fort Worth, and Arlington Police Department, Addison Police Department, and DPS, revealed that Mr. Candidate has never been arrested or convicted of any crime. The only entry in the Dallas Police Department's alpha file is when Mr. Candidate was six years old and fell down in front of his residence and was thought to be the victim of an auto accident. Copies of the returns are attached.

**MOTOR VEHICLE OPERATION**

**Driving Record**

Mr. Candidate's driving record revealed that he received two speeding citations in 1981 and has not received a citation since. Mr. Candidate was involved in one non-injury collision in 1984 and has had no subsequent collisions. A copy of Mr. Candidate's valid driver's license is attached.

## **GENERAL TOPICS**

### **Insurance**

Mr. Candidate has never had insurance refused or cancelled.

### **Other**

Checks revealed that Mr. Candidate has never belonged to any illegal organization and has no record of any substance abuse.

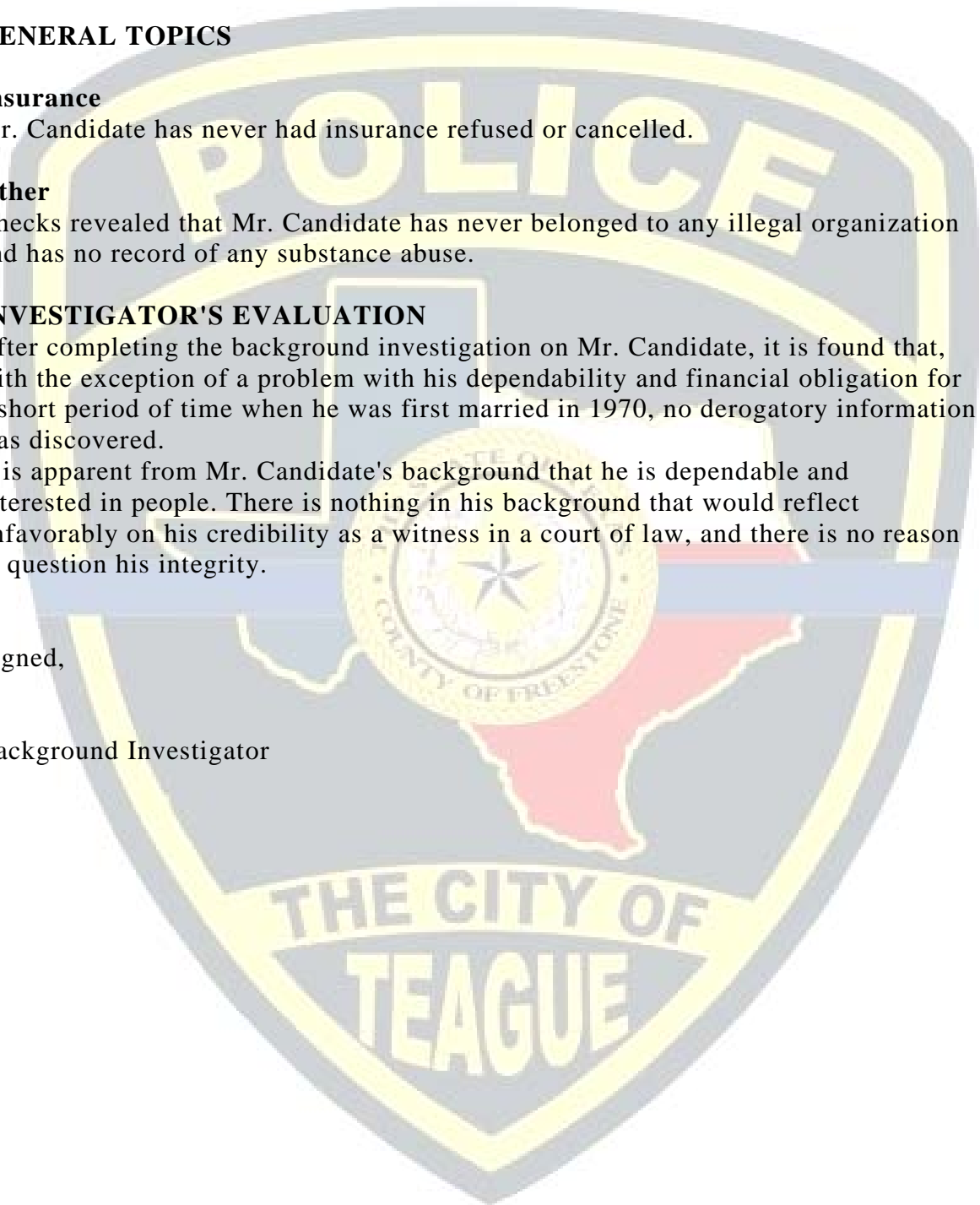
## **INVESTIGATOR'S EVALUATION**

After completing the background investigation on Mr. Candidate, it is found that, with the exception of a problem with his dependability and financial obligation for a short period of time when he was first married in 1970, no derogatory information was discovered.

It is apparent from Mr. Candidate's background that he is dependable and interested in people. There is nothing in his background that would reflect unfavorably on his credibility as a witness in a court of law, and there is no reason to question his integrity.

Signed,

Background Investigator



AUTHORIZATION FOR RELEASE OF  
PERSONAL INFORMATION

I, \_\_\_\_\_ do hereby authorize a review of and full disclosure of all records concerning myself to any duly authorized agent of the Teague Police Department whether the said records are private, public or confidential nature.

The intent of this authorization is to give my consent for full and complete disclosure of the records of educational institutions, financial or credit institutions, including records of loans, the records of commercial or retail, credit agencies (including credit reports and/or ratings); and other financial statements and records wherever filed; medical and psychiatric treatment and/or consultation, including hospitals, clinics, private practitioners and the U.S. Veteran's Administration; employment and pre-employment records, including background reports, efficiency ratings, complaints or grievances filed by or against me and the records and recollections of attorneys at law, or of other counsel, whether representing one or another person in any case, either criminal or civil, in which I presently have, or have had an interest in.

I understand that any information obtained by the Personal History Background investigation, which is developed directly or indirectly, in whole or in part, upon this release of authorization, will be considered in determining my suitability for employment or advancement by the Teague Police Department. I also certify that any person(s) who may furnish such information concerning me shall not be held accountable for giving this information; and I do hereby release said person(s) from any and all liability which may be incurred as a result of furnishing such information.

Information received from all sources will be kept confidential and will not be released to either the applicant or personnel not involved in the hiring/promotion process.

A photocopy of this release form will be valid as an original thereof, even though the said photocopy does not contain an original writing of my signature.

\_\_\_\_\_  
Signature (Includes maiden name if applicable)

Address: \_\_\_\_\_

Phone: (\_\_\_\_) \_\_\_\_\_

Date of Birth: \_\_\_\_\_

Social Security No. \_\_\_\_\_

Subscribed and sworn to before me, by the said: \_\_\_\_\_, This \_\_\_\_ day of \_\_\_\_\_, 20\_\_.

\_\_\_\_\_  
Notary Public In and For the State of Texas





# **Criminal Justice Information Services (CJIS) Security Policy**

Version 5.9  
06/01/2020

CJISD-ITS-DOC-08140-5.9



Prepared by:  
CJIS Information Security Officer

Approved by:  
CJIS Advisory Policy Board

## EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

## CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5	Policy Rewrite	Security Policy Working Group	2/9/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	7/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	8/9/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	8/4/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/6/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	6/1/2016	APB & Compact Council
5.6	Incorporate Calendar Year 2016 APB approved changes and administrative changes	CJIS ISO Program Office	6/5/2017	APB & Compact Council
5.7	Incorporate Calendar Year 2017 APB approved changes and administrative changes	CJIS ISO Program Office	08/16/2018	APB & Compact Council
5.8	Incorporate Calendar Year 2018 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2019	APB & Compact Council
5.9	Incorporate Calendar Year 2019 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2020	APB & Compact Council

## SUMMARY OF CHANGES

Version 5.9

### APB Approved Changes

1. **Section 5.13.2 Mobile Device Management (MDM):** add clarifying language, Fall 2019, APB#18, SA#3, Mobile Device Management (MDM) Requirements in the *CJIS Security Policy*.
2. **Appendix H, Security Addendum:** add example of contract addendum, Fall 2019, APB#18, SA#7, Audit of Vendor Contracts with Authorized Criminal Justice Agencies (CJAs).
3. **NOTE:** There were no Spring 2019 APB actions.

### Administrative Changes<sup>1</sup>

1. **Section 5.6.2.2.2 Advanced Authentication Decision Tree:** updated the tree description to account for direct and indirect access to CJI.
2. **Figures 9 and 10:** updated both figures to account for direct and indirect access to CJI.

KEY TO APB APPROVED CHANGES (e.g. “Fall 2013, APB#11, SA#6, add language, Future CSP for Mobile Devices”):

Fall 2013 – Advisory Policy Board cycle and year

APB# – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Summary of change

Topic title

---

<sup>1</sup> Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

# TABLE OF CONTENTS

<b>Executive Summary</b> .....	<b>i</b>
<b>Change Management</b> .....	<b>ii</b>
<b>Summary of Changes</b> .....	<b>iii</b>
<b>Table of Contents</b> .....	<b>iv</b>
<b>List of Figures</b> .....	<b>ix</b>
<b>1 Introduction</b> .....	<b>1</b>
1.1 Purpose .....	1
1.2 Scope .....	1
1.3 Relationship to Local Security Policy and Other Policies .....	1
1.4 Terminology Used in This Document .....	2
1.5 Distribution of the CJIS Security Policy .....	2
<b>2 CJIS Security Policy Approach</b> .....	<b>3</b>
2.1 CJIS Security Policy Vision Statement .....	3
2.2 Architecture Independent .....	3
2.3 Risk Versus Realism .....	3
<b>3 Roles and Responsibilities</b> .....	<b>4</b>
3.1 Shared Management Philosophy .....	4
3.2 Roles and Responsibilities for Agencies and Parties .....	4
3.2.1 CJIS Systems Agencies (CSA) .....	5
3.2.2 CJIS Systems Officer (CSO) .....	5
3.2.3 Terminal Agency Coordinator (TAC) .....	6
3.2.4 Criminal Justice Agency (CJA) .....	6
3.2.5 Noncriminal Justice Agency (NCJA) .....	6
3.2.6 Contracting Government Agency (CGA) .....	7
3.2.7 Agency Coordinator (AC) .....	7
3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO) .....	7
3.2.9 Local Agency Security Officer (LASO) .....	8
3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO) .....	8
3.2.11 Repository Manager .....	9
3.2.12 Compact Officer .....	9
<b>4 Criminal Justice Information and Personally Identifiable Information</b> .....	<b>10</b>
4.1 Criminal Justice Information (CJI) .....	10
4.1.1 Criminal History Record Information (CHRI) .....	10
4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information .....	11
4.2.1 Proper Access, Use, and Dissemination of CHRI .....	11
4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information .....	11
4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information .....	11
4.2.3.1 For Official Purposes .....	11
4.2.3.2 For Other Authorized Purposes .....	12
4.2.3.3 CSO Authority in Other Circumstances .....	12
4.2.4 Storage .....	12
4.2.5 Justification and Penalties .....	12

4.2.5.1	Justification .....	12
4.2.5.2	Penalties .....	12
4.3	Personally Identifiable Information (PII).....	12
<b>5</b>	<b>Policy and Implementation .....</b>	<b>14</b>
5.1	Policy Area 1: Information Exchange Agreements .....	15
5.1.1	Information Exchange .....	15
5.1.1.1	Information Handling.....	15
5.1.1.2	State and Federal Agency User Agreements .....	15
5.1.1.3	Criminal Justice Agency User Agreements .....	16
5.1.1.4	Interagency and Management Control Agreements .....	16
5.1.1.5	Private Contractor User Agreements and CJIS Security Addendum.....	16
5.1.1.6	Agency User Agreements .....	17
5.1.1.7	Outsourcing Standards for Channelers .....	17
5.1.1.8	Outsourcing Standards for Non-Channelers .....	18
5.1.2	Monitoring, Review, and Delivery of Services .....	18
5.1.2.1	Managing Changes to Service Providers .....	18
5.1.3	Secondary Dissemination.....	18
5.1.4	Secondary Dissemination of Non-CHRI CJI .....	18
5.2	Policy Area 2: Security Awareness Training.....	20
5.2.1	Basic Security Awareness Training .....	20
5.2.1.1	Level One Security Awareness Training .....	20
5.2.1.2	Level Two Security Awareness Training .....	20
5.2.1.3	Level Three Security Awareness Training .....	21
5.2.1.4	Level Four Security Awareness Training .....	21
5.2.2	LASO Training.....	22
5.2.3	Security Training Records.....	22
5.3	Policy Area 3: Incident Response .....	24
5.3.1	Reporting Security Events.....	24
5.3.1.1	Reporting Structure and Responsibilities.....	24
5.3.1.1.1	FBI CJIS Division Responsibilities .....	24
5.3.1.1.2	CSA ISO Responsibilities.....	24
5.3.2	Management of Security Incidents.....	25
5.3.2.1	Incident Handling.....	25
5.3.2.2	Collection of Evidence.....	25
5.3.3	Incident Response Training.....	25
5.3.4	Incident Monitoring.....	25
5.4	Policy Area 4: Auditing and Accountability.....	27
5.4.1	Auditable Events and Content (Information Systems).....	27
5.4.1.1	Events.....	27
5.4.1.1.1	Content.....	28
5.4.2	Response to Audit Processing Failures .....	28
5.4.3	Audit Monitoring, Analysis, and Reporting.....	28
5.4.4	Time Stamps.....	28
5.4.5	Protection of Audit Information .....	28
5.4.6	Audit Record Retention.....	28
5.4.7	Logging NCIC and III Transactions.....	29

5.5	Policy Area 5: Access Control.....	30
5.5.1	Account Management .....	30
5.5.2	Access Enforcement.....	30
5.5.2.1	Least Privilege .....	31
5.5.2.2	System Access Control .....	31
5.5.2.3	Access Control Criteria.....	31
5.5.2.4	Access Control Mechanisms.....	31
5.5.3	Unsuccessful Login Attempts .....	32
5.5.4	System Use Notification.....	32
5.5.5	Session Lock .....	32
5.5.6	Remote Access .....	33
5.5.6.1	Personally Owned Information Systems.....	33
5.5.6.2	Publicly Accessible Computers .....	33
5.6	Policy Area 6: Identification and Authentication .....	35
5.6.1	Identification Policy and Procedures.....	35
5.6.1.1	Use of Originating Agency Identifiers in Transactions and Information Exchanges .....	35
5.6.2	Authentication Policy and Procedures .....	35
5.6.2.1	Standard Authenticators.....	36
5.6.2.1.1	Password .....	36
5.6.2.1.2	Personal Identification Number (PIN) .....	38
5.6.2.1.3	One-time Passwords (OTP) .....	38
5.6.2.2	Advanced Authentication.....	38
5.6.2.2.1	Advanced Authentication Policy and Rationale .....	39
5.6.2.2.2	Advanced Authentication Decision Tree .....	39
5.6.3	Identifier and Authenticator Management .....	41
5.6.3.1	Identifier Management.....	41
5.6.3.2	Authenticator Management.....	42
5.6.4	Assertions .....	42
5.7	Policy Area 7: Configuration Management .....	48
5.7.1	Access Restrictions for Changes .....	48
5.7.1.1	Least Functionality.....	48
5.7.1.2	Network Diagram.....	48
5.7.2	Security of Configuration Documentation .....	48
5.8	Policy Area 8: Media Protection.....	49
5.8.1	Media Storage and Access .....	49
5.8.2	Media Transport .....	49
5.8.2.1	Digital Media during Transport .....	49
5.8.2.2	Physical Media in Transit .....	49
5.8.3	Digital Media Sanitization and Disposal.....	49
5.8.4	Disposal of Physical Media.....	49
5.9	Policy Area 9: Physical Protection .....	51
5.9.1	Physically Secure Location .....	51
5.9.1.1	Security Perimeter.....	51
5.9.1.2	Physical Access Authorizations .....	51
5.9.1.3	Physical Access Control .....	51

5.9.1.4	Access Control for Transmission Medium .....	51
5.9.1.5	Access Control for Display Medium .....	51
5.9.1.6	Monitoring Physical Access .....	52
5.9.1.7	Visitor Control .....	52
5.9.1.8	Delivery and Removal .....	52
5.9.2	Controlled Area .....	52
5.10	Policy Area 10: System and Communications Protection and Information Integrity .....	53
5.10.1	Information Flow Enforcement .....	53
5.10.1.1	Boundary Protection .....	53
5.10.1.2	Encryption.....	54
5.10.1.2.1	Encryption for CJI in Transit .....	54
5.10.1.2.2	Encryption for CJI at Rest.....	55
5.10.1.2.3	Public Key Infrastructure (PKI) Technology.....	55
5.10.1.3	Intrusion Detection Tools and Techniques .....	55
5.10.1.4	Voice over Internet Protocol.....	56
5.10.1.5	Cloud Computing.....	56
5.10.2	Facsimile Transmission of CJI.....	57
5.10.3	Partitioning and Virtualization .....	57
5.10.3.1	Partitioning.....	57
5.10.3.2	Virtualization .....	58
5.10.4	System and Information Integrity Policy and Procedures.....	58
5.10.4.1	Patch Management.....	58
5.10.4.2	Malicious Code Protection.....	59
5.10.4.3	Spam and Spyware Protection .....	59
5.10.4.4	Security Alerts and Advisories .....	59
5.10.4.5	Information Input Restrictions.....	60
5.11	Policy Area 11: Formal Audits .....	61
5.11.1	Audits by the FBI CJIS Division.....	61
5.11.1.1	Triennial Compliance Audits by the FBI CJIS Division .....	61
5.11.1.2	Triennial Security Audits by the FBI CJIS Division .....	61
5.11.2	Audits by the CSA.....	61
5.11.3	Special Security Inquiries and Audits .....	62
5.11.4	Compliance Subcommittees .....	62
5.12	Policy Area 12: Personnel Security .....	63
5.12.1	Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI .....	63
5.12.2	Personnel Termination .....	64
5.12.3	Personnel Transfer.....	64
5.12.4	Personnel Sanctions.....	64
5.13	Policy Area 13: Mobile Devices .....	66
5.13.1	Wireless Communications Technologies .....	66
5.13.1.1	802.11 Wireless Protocols .....	66
5.13.1.2	Cellular Devices.....	67
5.13.1.2.1	Cellular Service Abroad.....	68
5.13.1.2.2	Voice Transmissions Over Cellular Devices .....	68
5.13.1.3	Bluetooth.....	68



5.13.1.4	Mobile Hotspots.....	68
5.13.2	Mobile Device Management (MDM) .....	69
5.13.3	Wireless Device Risk Mitigations .....	69
5.13.4	System Integrity .....	70
5.13.4.1	Patching/Updates .....	70
5.13.4.2	Malicious Code Protection.....	70
5.13.4.3	Personal Firewall .....	70
5.13.5	Incident Response .....	71
5.13.6	Access Control .....	71
5.13.7	Identification and Authentication.....	71
5.13.7.1	Local Device Authentication .....	71
5.13.7.2	Advanced Authentication.....	72
5.13.7.2.1	Compensating Controls.....	72
5.13.7.3	Device Certificates.....	72
<b>Appendices.....</b>		<b>A-1</b>
<b>Appendix A</b>	<b>Terms and Definitions .....</b>	<b>A-1</b>
<b>Appendix B</b>	<b>Acronyms.....</b>	<b>B-1</b>
<b>Appendix C</b>	<b>Network Topology Diagrams .....</b>	<b>C-1</b>
<b>Appendix D</b>	<b>Sample Information Exchange Agreements.....</b>	<b>D-1</b>
D.1	CJIS User Agreement .....	D-1
D.2	Management Control Agreement.....	D-9
D.3	Noncriminal Justice Agency Agreement & Memorandum of Understanding.....	D-10
D.4	Interagency Connection Agreement .....	D-16
<b>Appendix E</b>	<b>Security Forums and Organizational Entities.....</b>	<b>E-1</b>
<b>Appendix F</b>	<b>Sample Forms.....</b>	<b>F-1</b>
F.1	Security Incident Response Form .....	F-2
<b>Appendix G</b>	<b>Best practices.....</b>	<b>G-1</b>
G.1	Virtualization .....	G-1
G.2	Voice over Internet Protocol.....	G-4
G.3	Cloud Computing.....	G-15
G.4	Mobile Appendix .....	G-32
G.5	Administrator Accounts for Least Privilege and Separation of Duties.....	G-53
G.6	Encryption.....	G-66
G.7	Incident Response .....	G-76
G.8	Secure Coding.....	G-89
<b>Appendix H</b>	<b>Security Addendum .....</b>	<b>H-1</b>
<b>Appendix I</b>	<b>References.....</b>	<b>I-1</b>
<b>Appendix J</b>	<b>Noncriminal Justice Agency Supplemental Guidance .....</b>	<b>J-1</b>
<b>Appendix K</b>	<b>Criminal Justice Agency Supplemental Guidance .....</b>	<b>K-1</b>

## LIST OF FIGURES

Figure 1 – Overview Diagram of Strategic Functions and Policy Components.....	4
Figure 2 – Dissemination of restricted and non-restricted NCIC data.....	13
Figure 3 – Information Exchange Agreements Implemented by a Local Police Department .....	19
Figure 4 – Security Awareness Training Use Cases.....	22
Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department .....	26
Figure 6 – Local Police Department's Use of Audit Logs .....	29
Figure 7 – A Local Police Department's Access Controls .....	34
Figure 8 – Advanced Authentication Use Cases.....	42
Figure 9 – Authentication Decision for Known Location .....	46
Figure 10 – Authentication Decision for Unknown Location .....	47
Figure 11 – A Local Police Department's Configuration Management Controls .....	48
Figure 12 – A Local Police Department's Media Management Policies.....	50
Figure 13 – A Local Police Department's Physical Protection Measures.....	52
Figure 14 – System and Communications Protection and Information Integrity Use Cases.....	60
Figure 15 – The Audit of a Local Police Department.....	62
Figure 16 – A Local Police Department's Personnel Security Controls .....	64

# 1 INTRODUCTION

---

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

## 1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

## 1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

## 1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies

and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

## **1.4 Terminology Used in This Document**

The following terms are used interchangeably throughout this document:

- **Agency and Organization:** The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- **Information and Data:** Both terms refer to CJI.
- **System, Information System, Service, or named applications like NCIC:** all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.
- **References/Citations/Directives:** Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

Appendix A and B provide an extensive list of the terms and acronyms.

## **1.5 Distribution of the CJIS Security Policy**

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

## **2 CJIS SECURITY POLICY APPROACH**

---

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

### **2.1 CJIS Security Policy Vision Statement**

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

### **2.2 Architecture Independent**

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Next Generation Identification (NGI) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

### **2.3 Risk Versus Realism**

Every “shall” statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

### 3 ROLES AND RESPONSIBILITIES

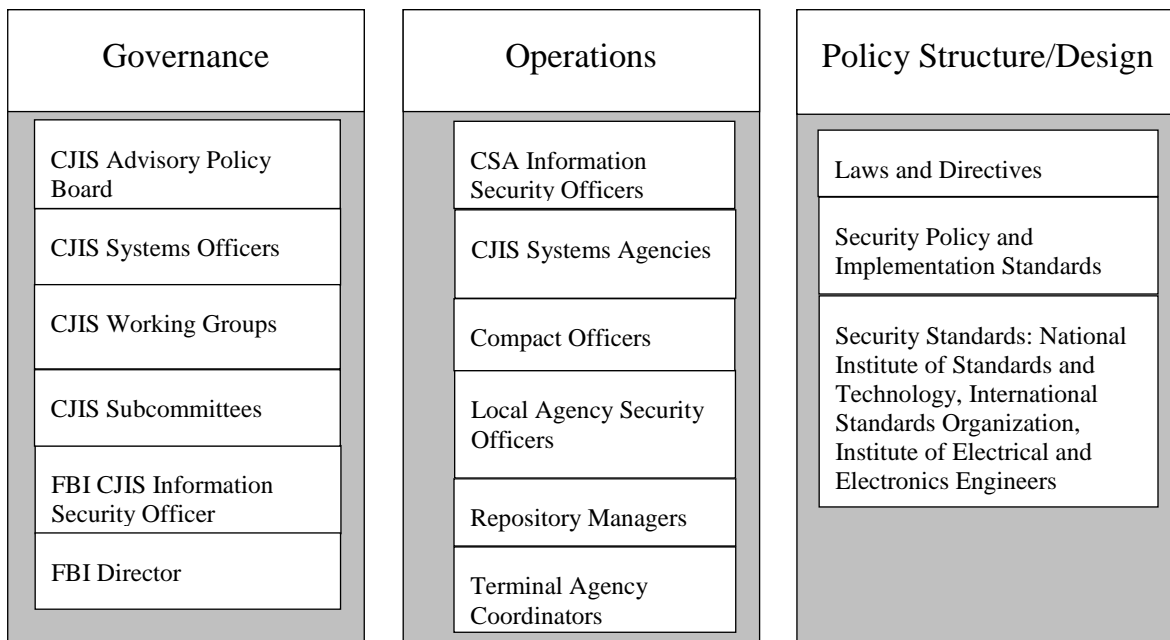
#### 3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

#### 3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.



**Figure 1 – Overview Diagram of Strategic Functions and Policy Components**

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

### **3.2.1 CJIS Systems Agencies (CSA)**

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

### **3.2.2 CJIS Systems Officer (CSO)**

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJIS.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJIS, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
  - a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
  - b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

- c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
  - d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with devices accessing CJIS systems.
  - e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
  - f. Ensure each LASO receives enhanced security awareness training (ref. Section 5.2).
  - g. Approve access to FBI CJIS systems.
  - h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
  - i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
3. Outsourcing of Criminal Justice Functions
- a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
  - b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

### **3.2.3 Terminal Agency Coordinator (TAC)**

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

### **3.2.4 Criminal Justice Agency (CJA)**

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

### **3.2.5 Noncriminal Justice Agency (NCJA)**

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.



### **3.2.6 Contracting Government Agency (CGA)**

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

### **3.2.7 Agency Coordinator (AC)**

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

### **3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)**

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

### **3.2.9 Local Agency Security Officer (LASO)**

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

### **3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)**

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA's ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

### **3.2.11 Repository Manager**

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

### **3.2.12 Compact Officer**

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

## 4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

---

### 4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding that can be released to the public via a public records request is not subject to the CJIS Security Policy.

#### 4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as “restricted data”, is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

## **4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information**

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

### **4.2.1 Proper Access, Use, and Dissemination of CHRI**

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

### **4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information**

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

### **4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information**

#### **4.2.3.1 For Official Purposes**

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with

the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

#### **4.2.3.2 For Other Authorized Purposes**

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

#### **4.2.3.3 CSO Authority in Other Circumstances**

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

#### **4.2.4 Storage**

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

#### **4.2.5 Justification and Penalties**

##### **4.2.5.1 Justification**

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

##### **4.2.5.2 Penalties**

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

### **4.3 Personally Identifiable Information (PII)**

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for

example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

**Figure 2 – Dissemination of restricted and non-restricted NCIC data**

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

## 5 POLICY AND IMPLEMENTATION

---

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices



## **5.1 Policy Area 1: Information Exchange Agreements**

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

### **5.1.1 Information Exchange**

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

#### **5.1.1.1 Information Handling**

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

#### **5.1.1.2 State and Federal Agency User Agreements**

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA

or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

#### **5.1.1.3 Criminal Justice Agency User Agreements**

Any CJA receiving access to CJIS shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

#### **5.1.1.4 Interagency and Management Control Agreements**

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJIS. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

#### **5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum**

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security

Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

#### **5.1.1.6 Agency User Agreements**

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

#### **5.1.1.7 Outsourcing Standards for Channelers**

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

#### **5.1.1.8 Outsourcing Standards for Non-Channelers**

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

### **5.1.2 Monitoring, Review, and Delivery of Services**

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

#### **5.1.2.1 Managing Changes to Service Providers**

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

### **5.1.3 Secondary Dissemination**

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

### **5.1.4 Secondary Dissemination of Non-CHRI CJI**

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

**Figure 3 – Information Exchange Agreements Implemented by a Local Police Department**

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

## **5.2 Policy Area 2: Security Awareness Training**

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

### **5.2.1 Basic Security Awareness Training**

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

#### **5.2.1.1 Level One Security Awareness Training**

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

#### **5.2.1.2 Level Two Security Awareness Training**

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

### **5.2.1.3 Level Three Security Awareness Training**

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical and logical access to CJJ:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating “shoulder surfing”), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

### **5.2.1.4 Level Four Security Awareness Training**

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.

3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

### 5.2.2 LASO Training

LASO training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

### 5.2.3 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

### Figure 4 – Security Awareness Training Use Cases

#### Use Case 1 - Security Awareness Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department’s entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

#### Use Case 2 - Level One Security Awareness Training

A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.

#### Use Case 3 – Level Two Security Awareness Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the



ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1 and 5.2.1.2.

Use Case 4 – Level Three Security Awareness Training

A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.

Use Case 5 – Level Four Security Awareness Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems, and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, 5.2.1.3, and 5.2.1.4.

## **5.3 Policy Area 3: Incident Response**

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

### **5.3.1 Reporting Security Events**

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

#### **5.3.1.1 Reporting Structure and Responsibilities**

##### **5.3.1.1.1 FBI CJIS Division Responsibilities**

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

##### **5.3.1.1.2 CSA ISO Responsibilities**

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

### **5.3.2 Management of Security Incidents**

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

#### **5.3.2.1 Incident Handling**

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

#### **5.3.2.2 Collection of Evidence**

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

### **5.3.3 Incident Response Training**

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

### **5.3.4 Incident Monitoring**

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

## Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJIS was compromised.

## **5.4 Policy Area 4: Auditing and Accountability**

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJJ.

### **5.4.1 Auditable Events and Content (Information Systems)**

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

#### **5.4.1.1 Events**

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
  - a. access permission on a user account, file, directory or other system resource;
  - b. create permission on a user account, file, directory or other system resource;
  - c. write permission on a user account, file, directory or other system resource;
  - d. delete permission on a user account, file, directory or other system resource;
  - e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
  - a. access the audit log file;

- b. modify the audit log file;
- c. destroy the audit log file.

#### **5.4.1.1.1 Content**

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

#### **5.4.2 Response to Audit Processing Failures**

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

#### **5.4.3 Audit Monitoring, Analysis, and Reporting**

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

#### **5.4.4 Time Stamps**

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

#### **5.4.5 Protection of Audit Information**

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

#### **5.4.6 Audit Record Retention**

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for

example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

#### **5.4.7 Logging NCIC and III Transactions**

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

#### **Figure 6 – Local Police Department's Use of Audit Logs**

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department's ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJJ processing application's logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO's suspicion.

## **5.5 Policy Area 5: Access Control**

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJIS.

### **5.5.1 Account Management**

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

### **5.5.2 Access Enforcement**

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.



### **5.5.2.1 Least Privilege**

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

### **5.5.2.2 System Access Control**

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

### **5.5.2.3 Access Control Criteria**

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

### **5.5.2.4 Access Control Mechanisms**

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

### **5.5.3 Unsuccessful Login Attempts**

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

### **5.5.4 System Use Notification**

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

1. the system use information is available and when appropriate, is displayed before granting access;
2. any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
3. the notice given to public users of the information system includes a description of the authorized uses of the system.

### **5.5.5 Session Lock**

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall

directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

### **5.5.6 Remote Access**

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

#### **5.5.6.1 Personally Owned Information Systems**

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

#### **5.5.6.2 Publicly Accessible Computers**

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

### **Figure 7 – A Local Police Department’s Access Controls**

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA’s CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client’s executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

## **5.6 Policy Area 6: Identification and Authentication**

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

### **5.6.1 Identification Policy and Procedures**

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

#### **5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges**

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

### **5.6.2 Authentication Policy and Procedures**

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not

further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

### **5.6.2.1 Standard Authenticators**

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

#### **5.6.2.1.1 Password**

When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in 5.6.2.1.1.1, OR follow the advanced password standards in 5.6.2.1.1.2.

NOTE: There is no option to combine or select particular options between the two separate lists below.

##### **5.6.2.1.1.1 Basic Password Standards**

When agencies elect to follow the basic password standards, passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

##### **5.6.2.1.1.2 Advanced Password Standards**

When agencies elect to follow the advanced password standards, passwords shall:

1. Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).
2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password.
3. Verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

- a. Passwords obtained from previous breach corpuses
  - b. Dictionary words
  - c. Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’)
  - d. Context-specific words, such as the name of the service, the username, and derivatives thereof
4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the “banned passwords” list.
  5. If the chosen password is found to be part of a “banned passwords” list, the Verifier shall:
    - a. Advise the subscriber that they need to select a different password,
    - b. Provide the reason for rejection, and
    - c. Require the subscriber to choose a different password.
  6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.
  7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.
  8. Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.
  9. Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.
    - a. The salt shall be at least 32 bits in length.
    - b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.

Note: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.
  10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.

#### **5.6.2.1.2 Personal Identification Number (PIN)**

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
  - a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

**EXCEPTION:** When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

#### **5.6.2.1.3 One-time Passwords (OTP)**

One-time passwords are considered a “something you have” token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance

#### **5.6.2.2 Advanced Authentication**

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as



network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to “activate” that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

#### **5.6.2.2.1 Advanced Authentication Policy and Rationale**

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

**EXCEPTION:**

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. **EXAMPLES:**

1. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
2. A user, irrespective of their location, accesses a State’s portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

#### **5.6.2.2.2 Advanced Authentication Decision Tree**

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Is the access to CJI direct access or indirect access?
  - a. If access is direct, proceed to question 2.
  - b. If access is indirect, decision tree is completed. AA is not required.
2. Can request’s physical originating location be determined?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 3.

- a. The IP address is attributed to a physical structure; or
- b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is “no”. Skip to question number 5.

3. Does request originate from within a physically secure location as described in Section 5.9.1?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 4.

- a. The IP address is attributed to a physically secure location; or
- b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

4. Are all required technical controls implemented at this location or at the controlling agency?

If either (a) or (b) below are true the answer to the above question is “yes”. Decision tree completed. AA is not required.

- a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or
- b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

5. Does request originate from an agency-controlled user device?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 6.

- a. The static IP address or MAC address can be traced to registered device; or
- b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

6. Is the agency managed user device associated with and located within a criminal justice conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is “yes”. Proceed to Figure 9 Step 4.

- a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or
- b. The certificate presented is associated with a device associated with a criminal justice conveyance; or
- c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is “no”. Proceed to question number 7.

7. Is the user device an agency-issued and controlled smartphone or tablet?

If both (a) and (b) below are true, the answer to the above question is “yes.” Proceed to question number 8.

- a. The law enforcement agency issued the device to an individual; and
- b. The device is subject to administrative management control of the issuing agency.

If either (a) or (b) above is false, then the answer is “no.” Decision tree completed. AA required.

8. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented?

If (a) and (b) below are true, the answer to the above question is “yes.” Decision tree completed. AA is not required.

- a. An agency cannot meet a requirement due to legitimate technical or business constraints; and
- b. The CSO has given written approval permitting temporary AA compensating controls to be implemented in lieu of the required AA control measures.

If either (a) or (b) above is false then the answer is “no.” Decision tree completed. AA required.

### **5.6.3 Identifier and Authenticator Management**

The agency shall establish identifier and authenticator management processes.

#### **5.6.3.1 Identifier Management**

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.

5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

### 5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

### 5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

## Figure 8 – Advanced Authentication Use Cases

### Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password ("something you know"), and a one-time password OTP ("something you have") from a hardware token to satisfy the requirement for advanced authentication. Once the detective's credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

### Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to Criminal Justice Information (CJI) then enters the proper username (identification) and password (“something you know”). Once prompted, the user connects the smart card (“something you have”) to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

### Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user’s agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP (“something you have”) then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

### Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password (“something you know”). Once that has been completed, a one-time password (OTP) is sent to the user’s agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user’s identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

#### Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user, is not listed under the user’s profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. The CJIS Security Policy requirements for RBA have been satisfied.

#### Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password (“something you know”). The RBA detects this computer has not previously been used by the user and is not listed under the user’s profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user’s profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user’s profile. Using this collected data, the RBA presents challenge/response questions when changes to the user’s profile are noted versus every time the user logs in.

#### Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user’s job functions.

An audit by the CSA identifies the agency's use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

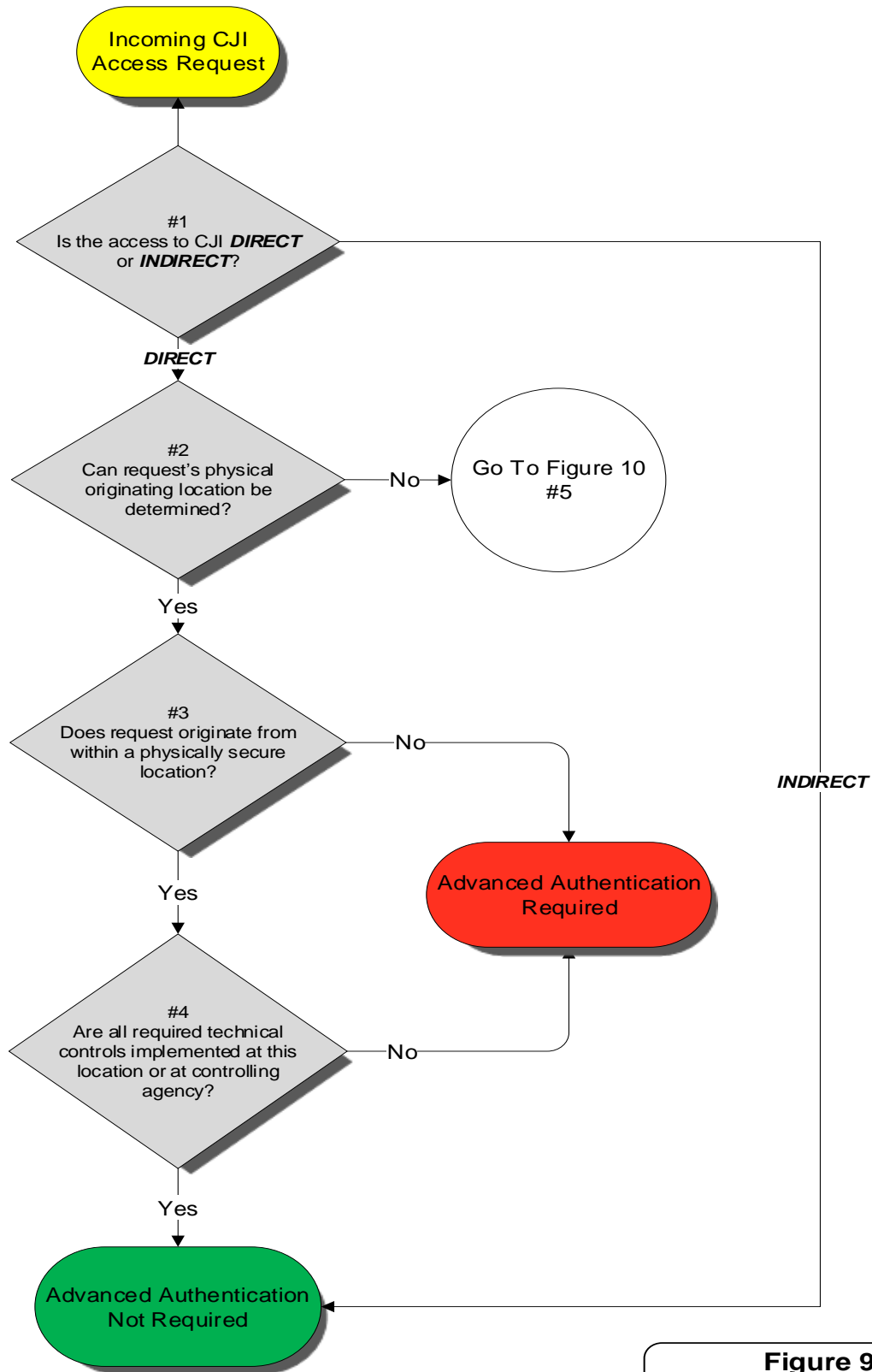
Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device
2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency's request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

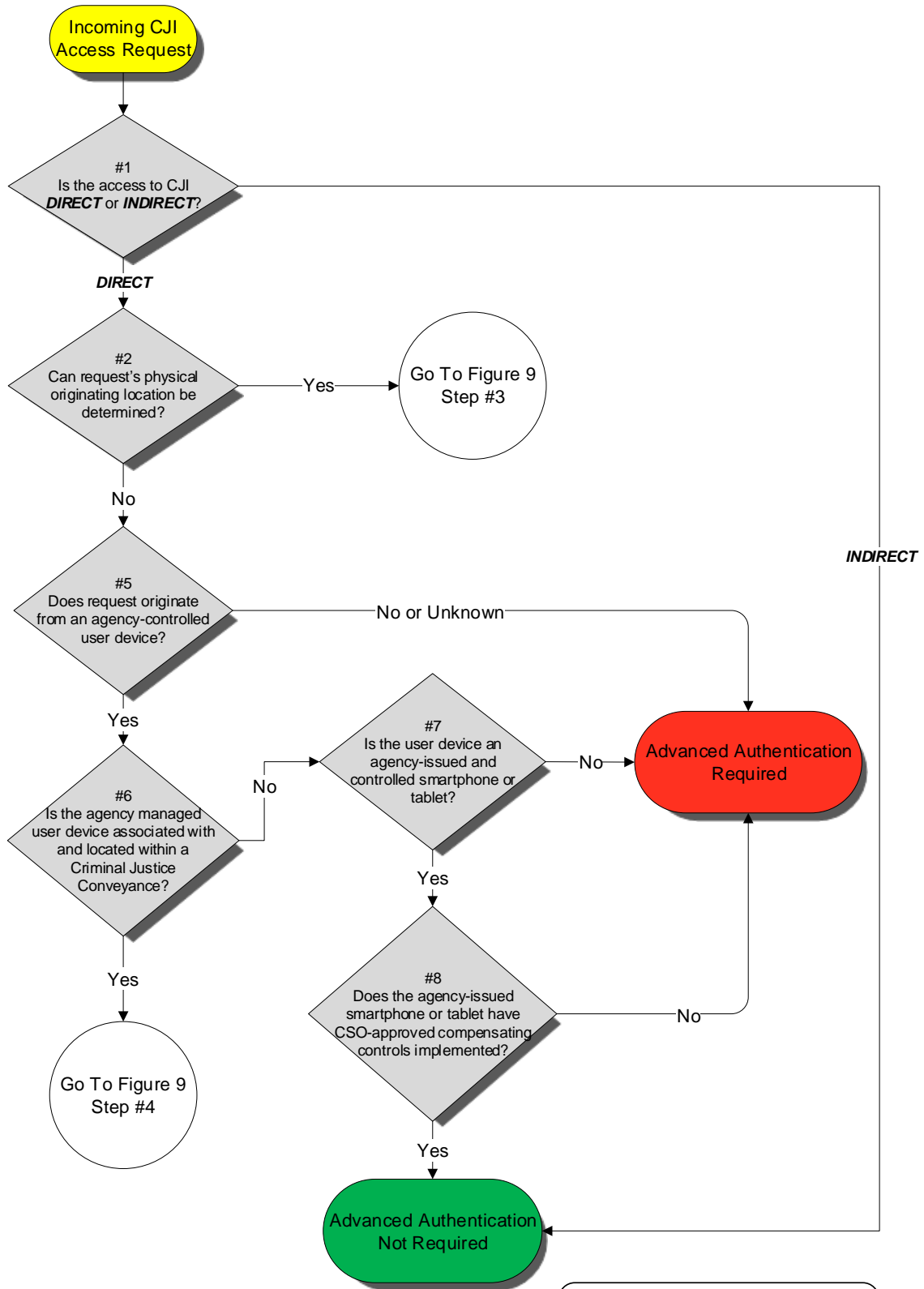
**Figure 9 – Authentication Decision for Known Location**



<b>Figure 9</b>		
	06/01/2020	



**Figure 10 – Authentication Decision for Unknown Location**



<b>Figure 10</b>		
	06/01/2020	

## **5.7 Policy Area 7: Configuration Management**

### **5.7.1 Access Restrictions for Changes**

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

#### **5.7.1.1 Least Functionality**

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

#### **5.7.1.2 Network Diagram**

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

### **5.7.2 Security of Configuration Documentation**

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

#### **Figure 11 – A Local Police Department’s Configuration Management Controls**

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

## **5.8 Policy Area 8: Media Protection**

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

### **5.8.1 Media Storage and Access**

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

### **5.8.2 Media Transport**

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

#### **5.8.2.1 Digital Media during Transport**

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

#### **5.8.2.2 Physical Media in Transit**

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

### **5.8.3 Digital Media Sanitization and Disposal**

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

### **5.8.4 Disposal of Physical Media**

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

## **Figure 12 – A Local Police Department’s Media Management Policies**

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor’s vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentiality of the police department’s data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor’s vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

## **5.9 Policy Area 9: Physical Protection**

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

### **5.9.1 Physically Secure Location**

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

#### **5.9.1.1 Security Perimeter**

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

#### **5.9.1.2 Physical Access Authorizations**

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

#### **5.9.1.3 Physical Access Control**

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

#### **5.9.1.4 Access Control for Transmission Medium**

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

#### **5.9.1.5 Access Control for Display Medium**

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

### **5.9.1.6 Monitoring Physical Access**

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

### **5.9.1.7 Visitor Control**

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

### **5.9.1.8 Delivery and Removal**

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

## **5.9.2 Controlled Area**

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

### **Figure 13 – A Local Police Department's Physical Protection Measures**

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state’s CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by criminal justice professionals. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems’ infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

## **5.10 Policy Area 10: System and Communications Protection and Information Integrity**

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

### **5.10.1 Information Flow Enforcement**

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

#### **5.10.1.1 Boundary Protection**

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

### **5.10.1.2 Encryption**

Encryption is a form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information. Decryption is the reversing of the cryptographic operation to convert the information back into a plaintext (readable) format. There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption). Hybrid encryption solutions do exist and use both asymmetric encryption for client/server certificate exchange – session integrity and symmetric encryption for bulk data encryption – data confidentiality.

#### **5.10.1.2.1 Encryption for CJI in Transit**

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

#### **EXCEPTIONS:**

1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
  - a. The agency owns, operates, manages, or protects the medium.
  - b. Medium terminates within physically secure locations at both ends with no interconnections between.
  - c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
  - d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
  - e. With prior approval of the CSO.

#### **Examples:**

- A campus is completely owned and controlled by a criminal justice agency (CJA)
  - If line-of-sight between buildings exists where a cable is buried, encryption is not required.



- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

#### **5.10.1.2.2 Encryption for CJI at Rest**

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
  - a. Be at least 10 characters
  - b. Not be a dictionary word.
  - c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
  - d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

#### **5.10.1.2.3 Public Key Infrastructure (PKI) Technology**

For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

1. Include authorization by a supervisor or a responsible official.
2. Be accomplished by a secure process that verifies the identity of the certificate holder.
3. Ensure the certificate is issued to the intended party.

#### **5.10.1.3 Intrusion Detection Tools and Techniques**

Intrusion detection systems are deployed inside a network to monitor events against a known set of parameters (i.e. malicious activity or policy violations) and make notification to the system of any event which violates any of those parameters. They are passive in nature, listening and

monitoring network traffic. There are mainly two types of IDS; network-based IDS (NIDS) and host-based IDS (HIDS).

Intrusion prevention systems are an IDS with the capability to respond to detected intrusions. They are normally deployed at the perimeter of a network, scanning traffic. Like detection systems, protection systems compare scanned traffic to defined normal parameters but unlike detection systems are able to take some type of immediate action to mitigate, or prevent, an event.

Agencies shall:

1. Implement network-based and/or host-based intrusion detection or prevention tools.
2. Maintain current intrusion detection or prevention signatures.
3. Monitor inbound and outbound communications for unusual or unauthorized activities.
4. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
5. Review intrusion detection or prevention logs weekly or implement automated event notification.
6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

#### **5.10.1.4 Voice over Internet Protocol**

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

#### **5.10.1.5 Cloud Computing**

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-

145, and 800-146), as well as the cloud provider’s policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its “intended use” is detailed within the service agreement. Such authorized uses of metadata may include, but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content – similar to Section 5.4), data usage/indexing metrics, and diagnostic/syslog data.

### **5.10.2 Facsimile Transmission of CJI**

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

### **5.10.3 Partitioning and Virtualization**

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

#### **5.10.3.1 Partitioning**

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.

2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

### **5.10.3.2 Virtualization**

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

## **5.10.4 System and Information Integrity Policy and Procedures**

### **5.10.4.1 Patch Management**

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

#### **5.10.4.2 Malicious Code Protection**

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

#### **5.10.4.3 Spam and Spyware Protection**

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

#### **5.10.4.4 Security Alerts and Advisories**

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.

5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

#### 5.10.4.5 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

### Figure 14 – System and Communications Protection and Information Integrity Use Cases

#### Use Case 1 – A Local Police Department’s Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state’s CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

#### Use Case 2 – Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

#### Use Case 3 – Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

## **5.11 Policy Area 11: Formal Audits**

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

### **5.11.1 Audits by the FBI CJIS Division**

#### **5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division**

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

#### **5.11.1.2 Triennial Security Audits by the FBI CJIS Division**

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

### **5.11.2 Audits by the CSA**

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.

### **5.11.3 Special Security Inquiries and Audits**

All agencies having access to CJIS shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

### **5.11.4 Compliance Subcommittees**

The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) established the Compliance Evaluation Subcommittee (CES) to evaluate the results of audits conducted by the CJIS Audit Unit (CAU). The CES makes specific recommendations to the APB concerning compliance with applicable policies and regulations. The most current information regarding the CAU audits that are within the purview of the CES and detailed CES sanctions process procedures are available at [CJIS.gov](http://CJIS.gov) (Law Enforcement Enterprise Portal) CJIS Special Interest Groups CES Section and CJIS Section of [FBI.gov](http://FBI.gov).

The National Crime Prevention and Privacy Compact (Compact) Council at Article VI established the Compact Council (Council). The Compact Council Sanctions Committee is responsible for ensuring the use of the Interstate Identification Index System for noncriminal justice purposes complies with the Compact and with rules, standards, and procedures established by the Compact Council. As such, the Sanctions Committee reviews the results of audits conducted by the Federal Bureau of Investigation (FBI) of participants in the FBI's Criminal Justice Services (CJIS) Division programs. The Sanctions Committee reviews the audit results and the participant's response to determine a course of action necessary to bring the participant into compliance and make recommendations to the Compact Council or the FBI. Additional information on the Compact Council Sanctions process is available on the Compact Council's web-site.

### **Figure 15 – The Audit of a Local Police Department**

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJIS. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJIS. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.



## 5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

### 5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:
  - a. 5 CFR 731.106; and/or
  - b. Office of Personnel Management policy, regulations, and guidance; and/or
  - c. agency policy, regulations, and guidance.

Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.
3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.
  - a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.
  - b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.
  - c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.

4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

### **5.12.2 Personnel Termination**

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.

### **5.12.3 Personnel Transfer**

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

### **5.12.4 Personnel Sanctions**

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

## **Figure 16 – A Local Police Department's Personnel Security Controls**

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated

policies. The police department re-evaluated each person's suitability for access to CJI every five years.

## **5.13 Policy Area 13: Mobile Devices**

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

### **5.13.1 Wireless Communications Technologies**

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

#### **5.13.1.1 802.11 Wireless Protocols**

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

#### **5.13.1.2 Cellular Devices**

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and “aircards” are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

### **5.13.1.2.1 Cellular Service Abroad**

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency’s policies prior to and after deployment outside of the U.S.

### **5.13.1.2.2 Voice Transmissions Over Cellular Devices**

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

### **5.13.1.3 Bluetooth**

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency’s operational and business processes.

### **5.13.1.4 Mobile Hotspots**

Many mobile devices include the capability to function as a WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot’s default SSID
  - a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot’s port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

### **5.13.2 Mobile Device Management (MDM)**

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full-featured operating systems may not function properly on devices with limited-feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. User agencies shall implement the following controls when directly accessing CJI from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the following controls:
  - a. Remote locking of device
  - b. Remote wiping of device
  - c. Setting and locking device configuration
  - d. Detection of “rooted” and “jailbroken” devices
  - e. Enforcement of folder or disk level encryption
  - f. Application of mandatory policy settings on the device
  - g. Detection of unauthorized configurations
  - h. Detection of unauthorized software or applications
  - i. Ability to determine the location of agency controlled devices
  - j. Prevention of unpatched devices from accessing CJI or CJI systems
  - k. Automatic device wiping after a specified number of failed access attempts

**EXCEPTION:** An MDM is not required when receiving CJI from an indirect access information system (i.e. the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.

### **5.13.3 Wireless Device Risk Mitigations**

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

2. Are configured for local device authentication (see Section 5.13.7.1).
3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

#### **5.13.4 System Integrity**

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM, application, or supporting service infrastructure.

##### **5.13.4.1 Patching/Updates**

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

##### **5.13.4.2 Malicious Code Protection**

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

##### **5.13.4.3 Personal Firewall**

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.



2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited-feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full-feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

### **5.13.5 Incident Response**

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
  - a. Device known to be locked, minimal duration of loss
  - b. Device lock state unknown, minimal duration of loss
  - c. Device lock state unknown, extended duration of loss
  - d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

### **5.13.6 Access Control**

Multiple user accounts are not generally supported on limited-feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

### **5.13.7 Identification and Authentication**

Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.

#### **5.13.7.1 Local Device Authentication**

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

### **5.13.7.2 Advanced Authentication**

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required.

#### **5.13.7.2.1 Compensating Controls**

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited-feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls
4. Expire upon the CSO approved date or when a compliant AA solution is implemented.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The compensating controls for AA are a combination of controls providing acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

The following minimum controls shall be implemented as part of the CSO approved compensating controls:

- Possession and registration of an agency issued smartphone or tablet as an indication it is the authorized user
- Use of device certificates per Section 5.13.7.3 Device Certificates
- Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored

#### **5.13.7.3 Device Certificates**

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

# APPENDICES

## APPENDIX A TERMS AND DEFINITIONS

---

**Access to Criminal Justice Information** — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

**Administration of Criminal Justice** — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

**Agency Controlled Mobile Device** — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJJ. The device can be agency issued or BYOD (personally owned).

**Agency Coordinator (AC)** — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

**Agency Issued Mobile Device** — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJJ. The device is not BYOD (personally owned).

**Agency Liaison (AL)** — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

**Asymmetric Encryption** — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

**Authorized User/Personnel** — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJJ.

**Authorized Recipient** — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

**Availability** — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

**Biographic Data** — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

**Biometric Data** — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

**Case / Incident History** — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

**Certificate Authority (CA) Certificate** – Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

**Channeler** — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

**Cloud Client** – A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

**Cloud Computing** – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

**Cloud Provider** – An organization that provides cloud computing services.

**Cloud Subscriber** – A person or organization that is a customer of a cloud computing service provider.

**CJIS Advisory Policy Board (APB)** — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

**CJIS Audit Unit (CAU)** — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy.

**CJIS Security Policy** — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

**CJIS Systems Agency (CSA)** — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS

Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

**CJIS Systems Agency Information Security Officer (CSA ISO)** — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

**CJIS Systems Officer (CSO)** — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

**Compact Council** — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

**Compact Officers** — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

**Compensating Controls** — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

**Computer Security Incident Response Capability (CSIRC)** — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

**Confidentiality** — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

**Contractor** — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

**Contracting Government Agency (CGA)** — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

**Crime Reports Data** — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

**Criminal History Record Information (CHRI)** — A subset of CJ. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

**Criminal Justice Agency (CJA)** — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

**Criminal Justice Agency User Agreement** — A terms-of-service agreement that must be signed prior to accessing CJ. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

**Criminal Justice Conveyance** — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

**Criminal Justice Information (CJI)** — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

**Criminal Justice Information Services Division (FBI CJIS or CJIS)** — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

**Data** — See Information and CJI.

**Decryption** – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

**Degauss** — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

**Department of Justice (DoJ)** — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

**Digital Media** – Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

**Digital Signature** – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message’s claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

**Direct Access** — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

**Dissemination** — The transmission/distribution of CJI to Authorized Recipients within an agency.

**Encryption** – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

**Escort** – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

**Facsimile (Fax)** – Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

**Federal Bureau of Investigation (FBI)** — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

**FBI CJIS Information Security Officer (FBI CJIS ISO)** — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA’s ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

**Federal Information Security Management Act (FISMA)** — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information

security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

**For Official Use Only (FOUO)** — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

**Full-feature Operating System** — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or “harden”, these devices from malicious network based technical attacks (e.g. malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

**Guest Operating System** — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

**Hashing** — The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e. hash value) to be used as a representative of that data.

**Hash Value** — The term that refers to an alphanumeric value which represents the result of applying a cryptographic hash function to data.

**Host Operating System** — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

**Hybrid Encryption** — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

**Hypervisor** — See Host Operating System.

**Identity History Data** — Textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.

**In-Band** – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

**Indirect Access** – Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

**Information** — See data and CJI.

**Information Exchange Agreement** — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party’s information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which



establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

**Information Security Officer (ISO)** — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

**Information System** — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

**Integrated Automated Fingerprint Identification System (IAFIS)** — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

**Integrity** — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

**Interconnection Security Agreement (ISA)** — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

**Interface Agency** — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

**Internet Protocol (IP)** — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

**Interstate Identification Index (III)** — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

**Intrusion Detection** — The process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents.

**Intrusion Detection System** — Software which automates the intrusion detection process.

**Intrusion Prevention** — The process of monitoring events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

**Intrusion Prevention System** — Software which has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

**Jailbreak (Jailbroken)** — The process of attaining privileged control (known as “root access”) of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

**Laptop Devices** – Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited-feature operating system (e.g. tablets).

**Law Enforcement Enterprise Portal (LEEP)** — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

**Limited-feature Operating System** — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). These operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited-feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

**Logical Access** – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

**Logical Partitioning** – When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

**Local Agency Security Officer (LASO)** — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

**Management Control Agreement (MCA)** — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA’s authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

**Metadata** — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.

**Mobile Device** — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

**Mobile Device Management (MDM)** — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

**Mobile (WiFi) Hotspot** — A mobile (WiFi) hotspot is a zone or area associated with a mobile device (e.g. smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

**National Crime Information Center (NCIC)** — An information system which stores CJJ which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

**National Instant Criminal Background Check System (NICS)** — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

**National Institute of Standards and Technology (NIST)** — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

**Noncriminal Justice Agency (NCJA)** — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

**NCJA (Government)** — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

**NCJA (Private)** — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would include a local bank.

**NCJA (Public)** — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJJ. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

**Noncriminal Justice Purpose** — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

**Office of Management and Budget (OMB)** — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the

supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

**One-time Password** — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.

**Out-of-Band** — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

**Outsourcing** — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

**Outsourcing Standard** — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

**Partitioning** – Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

**Password Verifier (Verifier)** – An entity or process that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

**Personal Firewall** — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

**Personally Identifiable Information (PII)** — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

**Physical Access** – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

**Physical Media** – Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

**Physical Partitioning** – When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

**Physically Secure Location** — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

**Pocket/Handheld Mobile Device** – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system

with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

**Property Data** — Information about vehicles and property associated with a crime.

**Rap Back** — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

**Receive-Only Terminal (ROT)** – A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

**Repository Manager, or Chief Administrator** — The designated manager of the agency having oversight responsibility for a CSA’s fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

**Root (Rooting, Rooted)** — The process of attaining privileged control (known as “root access”) of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

**Salting** –The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.

**Secondary Dissemination** — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

**Security Addendum (SA)** — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

**Sensitive But Unclassified (SBU)** — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

**Server/Client Computer Certificate (device-based)** – Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

**Service** — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

**Shredder** — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

**Smartphone** – See pocket/handheld mobile devices.

**Social Engineering** — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

**Software Patch** — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

**State and Federal Agency User Agreement** — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

**State Compact Officer** — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

**State Identification Bureau (SIB)** — The state agency with the responsibility for the state's fingerprint identification services.

**State Identification Bureau (SIB) Chief** — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

**State of Residency** – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

**Symmetric Encryption** — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

**System** — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to

applications and all interconnecting infrastructure required to use those applications that process CJJ.

**Tablet Devices** – Tablet devices are mobile devices with a limited-feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

**Terminal Agency Coordinator (TAC)** — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

**User Certificate (user-based)** – Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

**Virtual Escort** – Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

**Virtual Machine (VM)** – See Guest Operating System

**Virtualization** — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

**Voice over Internet Protocol (VoIP)** — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

**Wireless Access Point** – A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJJ.

**Wireless (WiFi) Hotspot** – A wireless (WiFi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

## APPENDIX B ACRONYMS

---

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice



DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle

MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau

SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
UCN	Universal Control Number
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

## **APPENDIX C NETWORK TOPOLOGY DIAGRAMS**

---

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJ, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

### Overview: Conceptual Connections Between Various Agencies

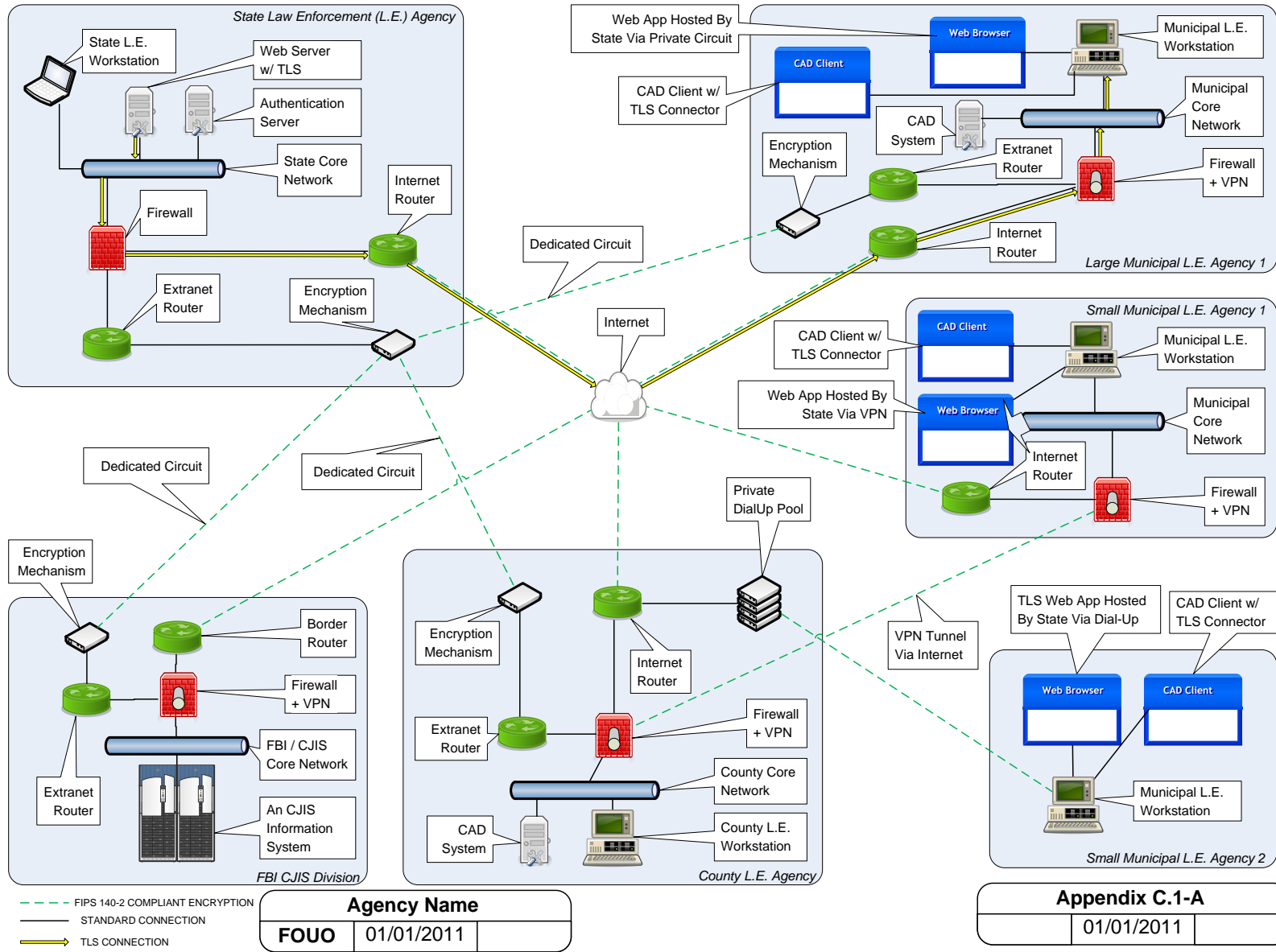
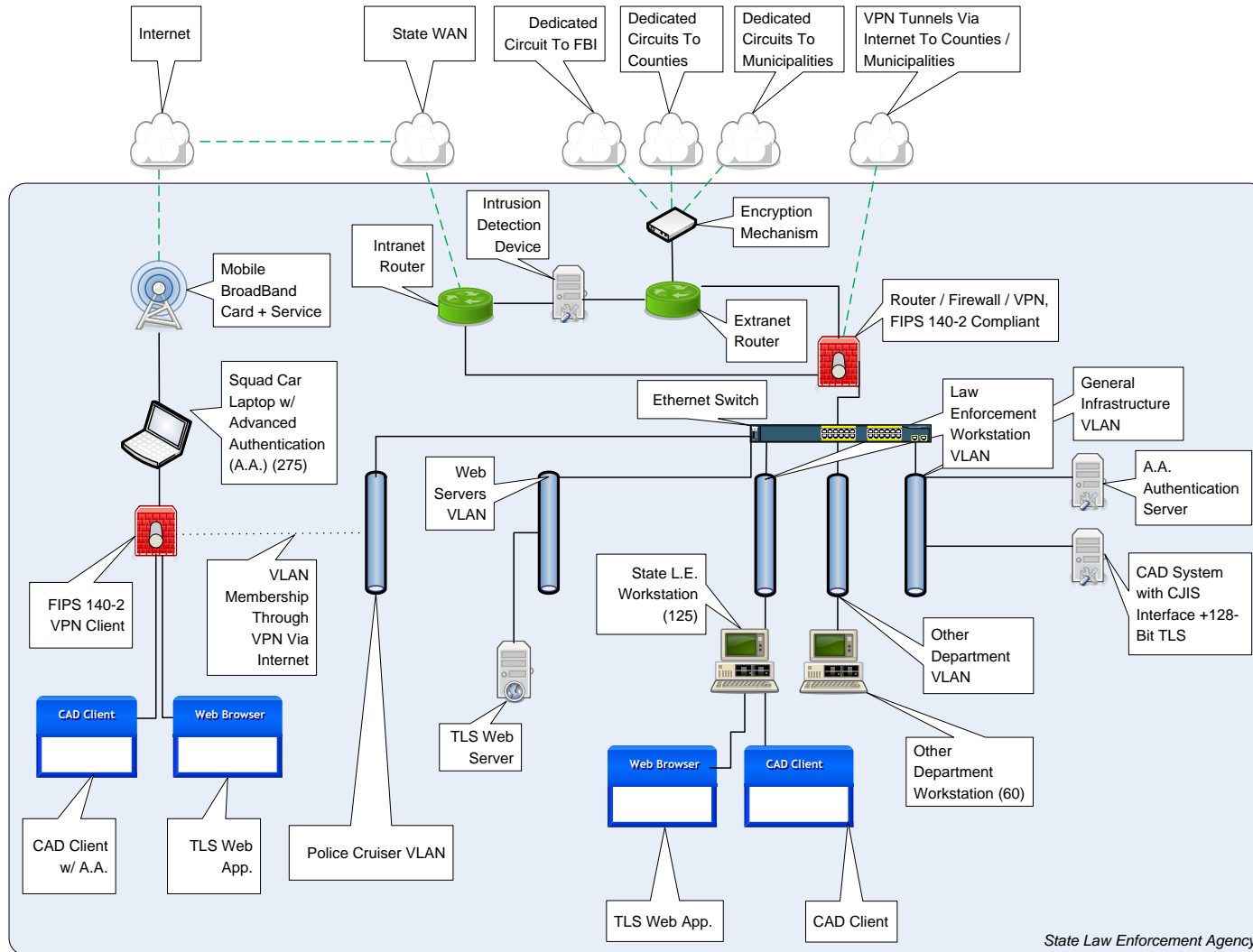


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

## Conceptual Topology Diagram For A State Law Enforcement Agency



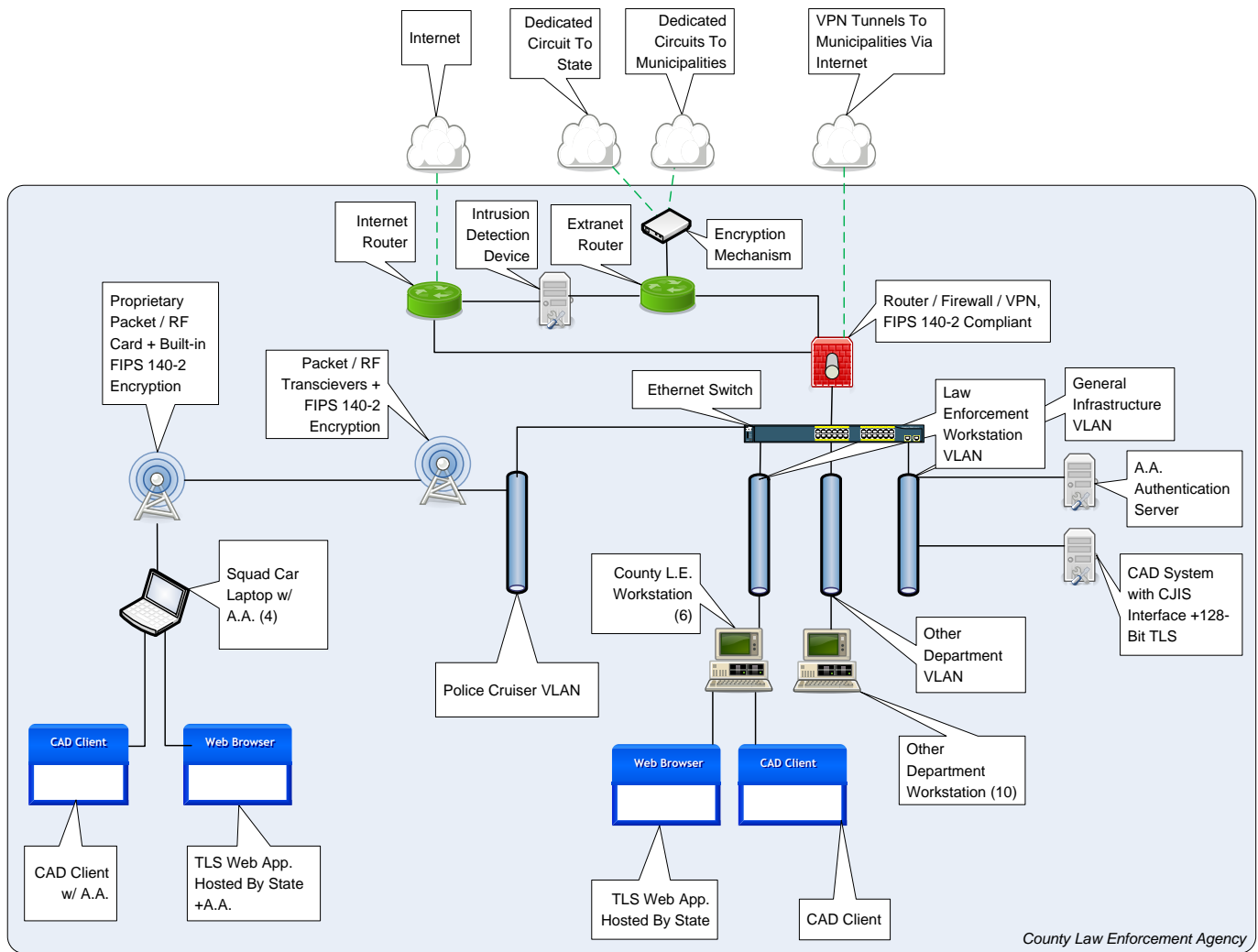
--- FIPS 140-2 COMPLIANT ENCRYPTION  
 ——— STANDARD CONNECTION

Sample State Agency		
FOUO	01/01/2011	

Appendix C.1-B		
	01/01/2011	

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

### Conceptual Topology Diagram For A County Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION  
 — STANDARD CONNECTION

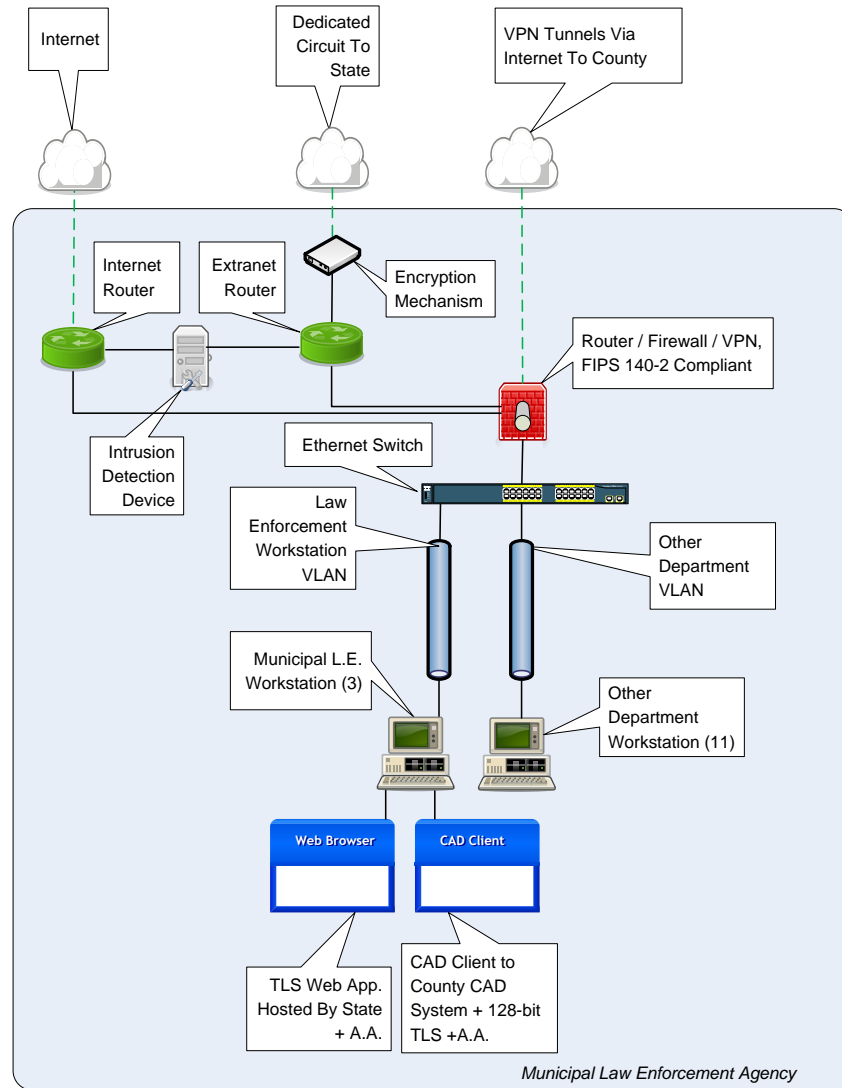
<b>Sample County Agency</b>		
<b>FOUO</b>	01/01/2011	

<b>Appendix C.1-C</b>		
	01/01/2011	



Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency

## Conceptual Topology Diagram For A Municipal Law Enforcement Agency



--- FIPS 140-2 COMPLIANT ENCRYPTION  
 ——— STANDARD CONNECTION

<b>Sample Municipal Agency</b>		
<b>FOUO</b>	01/01/2011	

<b>Appendix C.1-D</b>		
	01/01/2011	

# APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

---

## D.1 CJIS User Agreement

### CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Enterprise Portal; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.
2. Telecommunication lines to state, federal, and regulatory interfaces.
3. Legal and legislative review of matters pertaining to all CJIS Systems.
4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.
5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.
6. Ongoing assistance to Systems' users through meetings and briefings with the CSOs, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.
7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.
9. Annual NICS Users Conference.
10. Audit.
11. Staff research assistance.

## **PART 1**

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.
2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.
3. Biannual file synchronization of information entered into the III by participating states.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history

records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.
6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.
7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJ. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.
2. CJIS Security Policy.
3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.
4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.
5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.
6. The National Fingerprint File Qualification Requirements.
7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.
8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.
10. Applicable federal, state, and tribal laws and regulations.

## **PART 2**

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.
2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.
3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.
4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.
2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.
3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.
4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

## **GENERAL PROVISIONS**

### Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

### Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.
2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.
3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:
  - a. The parties will continue participation, financial or otherwise, up to the effective date of termination.
  - b. Each party will pay the costs it incurs as a result of termination.
  - c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

## **ACKNOWLEDGMENT AND CERTIFICATION**

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity. Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

**SYSTEMS USER AGREEMENT**

Please execute either Part 1 or Part 2

**PART 1**

\_\_\_\_\_ Date: \_\_\_\_\_  
CJIS Systems Officer  
\_\_\_\_\_  
Printed Name/Title

CONCURRENCE OF CSA HEAD:  
\_\_\_\_\_ Date: \_\_\_\_\_  
CSA Head  
\_\_\_\_\_  
Printed Name/Title

**PART 2**

\_\_\_\_\_ Date: \_\_\_\_\_  
CJIS WAN Official (or other CJIS Authorized Official)  
\_\_\_\_\_  
Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:  
\_\_\_\_\_ Date: \_\_\_\_\_  
CJIS WAN Agency Head  
\_\_\_\_\_  
Printed Name/Title



**FBI CJIS DIVISION:**

\_\_\_\_\_

Date: \_\_\_\_\_

[Name]

Assistant Director

FBI CJIS Division

\* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

## D.2 Management Control Agreement

### Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

- (1) Priorities.
- (2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
- (3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
- (4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
- (5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

“...management control of the criminal justice function remains solely with the Criminal Justice Agency.” Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

\_\_\_\_\_  
John Smith, CIO  
Any State Department of Administration

\_\_\_\_\_  
Date

\_\_\_\_\_  
Joan Brown, CIO  
(Criminal Justice Agency)

\_\_\_\_\_  
Date

## D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

**(Insert Name of Requesting Organization)**

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF  
THIRD-PARTY CONNECTIVITY TO THE  
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. **PURPOSE:** This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.
2. **BACKGROUND:** The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. **AUTHORITY:** The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. **SCOPE:**

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization's connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization's third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization's designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization's site.

v. Perform periodic monitoring and troubleshooting of the requesting organization's CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division's Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization's dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization's name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. **FUNDING:** There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. **SETTLEMENT OF DISPUTES:** Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

---

[Name]

---

Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

---

Date



## **D.4 Interagency Connection Agreement**

### **CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)**

#### **Wide Area Network (WAN) USER AGREEMENT**

#### **BY INTERIM REMOTE LATENT USERS**

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;
- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.
2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.
3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.
4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone

devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.
6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.
7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.



**FBI CJIS DIVISION:**

\_\_\_\_\_  
Signature – [Name]

Assistant Director \_\_\_\_\_  
Title Date

\* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

## APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

---

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC) <sup>2</sup>
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

## **APPENDIX F    SAMPLE FORMS**

---

This appendix contains sample forms.

## F.1 Security Incident Response Form

**FBI CJIS DIVISION  
INFORMATION SECURITY OFFICER (ISO)  
SECURITY INCIDENT REPORTING FORM**

---

NAME OF PERSON REPORTING THE INCIDENT: \_\_\_\_\_

DATE OF REPORT: \_\_\_\_\_ (mm/dd/yyyy)

DATE OF INCIDENT: \_\_\_\_\_ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): \_\_\_\_\_

---

LOCATION(S) OF INCIDENT: \_\_\_\_\_

INCIDENT DESCRIPTION: \_\_\_\_\_

---

SYSTEM(S) AFFECTED: \_\_\_\_\_

---

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): \_\_\_\_\_

---

METHOD OF DETECTION: \_\_\_\_\_

ACTIONS TAKEN/RESOLUTION: \_\_\_\_\_

---

**Copies To:**

**John C. Weatherly**

(FBI CJIS Division ISO)

1000 Custer Hollow Road

Clarksburg, WV 26306-0102

(304) 625-3660

[iso@fbi.gov](mailto:iso@fbi.gov)



# APPENDIX G BEST PRACTICES

---

## G.1 Virtualization

### Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>:

*“Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure.”*

From a trade publication, kernelthread.com

<http://www.kernelthread.com/publications/virtualization/>:

*“Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others.”*

From an Open Source Software developer

<http://www.kallasoft.com/pc-hardware-virtualization-basics/>:

*“Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:*

- *“Type-1 Hypervisor, which runs ‘bare-metal’ (on top of the hardware)*
- *“Type-2 Hypervisor which requires a separate application to run within an operating system*

*“Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system.”*

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on [www.virtualization.com](http://www.virtualization.com) are examples of industry offerings.

*“Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Server 2008 Hyper-V, and is fully supported by both companies’ channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments.”*

*“Sun Microsystems today announce the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for Sun xVM Server software and contribute to the direction and development of the product.”*

*“NetEx, specialist in high-speed data transport over TCP, today announced Virtual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide-area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company’s award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network.”*

From several sources, particularly:

<http://www.windowsecurity.com/articles/security-virtualization.html>

<http://csrc.nist.gov/publications/drafts/6--64rev2/draft-sp800-64-Revision2.pdf>

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply “least privilege” technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

## G.2 Voice over Internet Protocol

### Voice over Internet Protocol (VoIP)

#### Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

#### Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

#### Summary:

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

- a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.
- b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

- a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.
- b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

### **VoIP Risks, Threats, and Vulnerabilities**

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic “CIA”). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

#### Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker’s job easier.

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

#### Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

**REMEDIATION:** If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

#### Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

**REMEDIATION:** A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

#### ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

**REMEDIATION:** Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

#### Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDICATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

### IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDICATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

### Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDICATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

### Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

#### DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDICATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

#### TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious



information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

**REMEDIATION:** Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

### Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

#### CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

**REMEDIATION:** The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

#### Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root/root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

**REMEDIATION:** Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

### Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

**REMEDIATION:** These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

### Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

**REMEDIATION:** If remote access is not available, this problem can be solved with physical access control.

## **NIST Recommendations.**

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

### 1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.
- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.
- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling).
- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.
- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer

and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of

the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

## G.3 Cloud Computing

### Cloud Computing

#### Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

#### Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

#### Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

#### Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

### **Achieving CJIS Security Policy Compliance:**

The question that is often asked is, “Can an Agency be compliant with the CJIS Security Policy and also cloud compute?”

Because the CJIS Security Policy is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.



## General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)
- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)
- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)
- Are the encryption requirements being met? (5.10.1.2 Encryption)
  - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
  - Is the data encrypted while at rest and in transit?
- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
  - Will the cloud subscriber be notified of any incident?
  - If CJI is compromised, what are the notification and response procedures?
- Is the cloud service provider a private contractor/vendor?
  - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)
- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? *Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.* (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)

- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
  - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
  - What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

### Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment—Key Management Control, Security Awareness Training, and Personnel Controls

Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training (CJIS Security Policy section 5.2) and must meet personnel security (CJIS Security Policy Section 5.12) requirements as individuals with unescorted access to unencrypted CJI.

*Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI. However, it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task.*

- a. Scenario 1—Agency Stores CJI in a Cloud:

A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine, and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

- b. Scenario 2—Agency Accesses CJI While in a Cloud:

A CJA stores CJI (files and drives) in a cloud service provider's environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

c. Scenario 3–CJI Impact from a Cloud Datacenter Critical Systems Crash–Core Dump<sup>2</sup> Recovery:

A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider's administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

*Note: Writing encrypted data to a core dump corrupts the data and makes it unusable because the key no longer decrypts the data. This is problematic when attempting to recover encrypted data written to a core dump. The CJA could have ensured the cloud provider exclude encrypted data (CJI) from the core dump, but chose against it.*

### **The Cloud Model Explained:**

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

---

<sup>2</sup> Core Dump - A file of a computer's documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

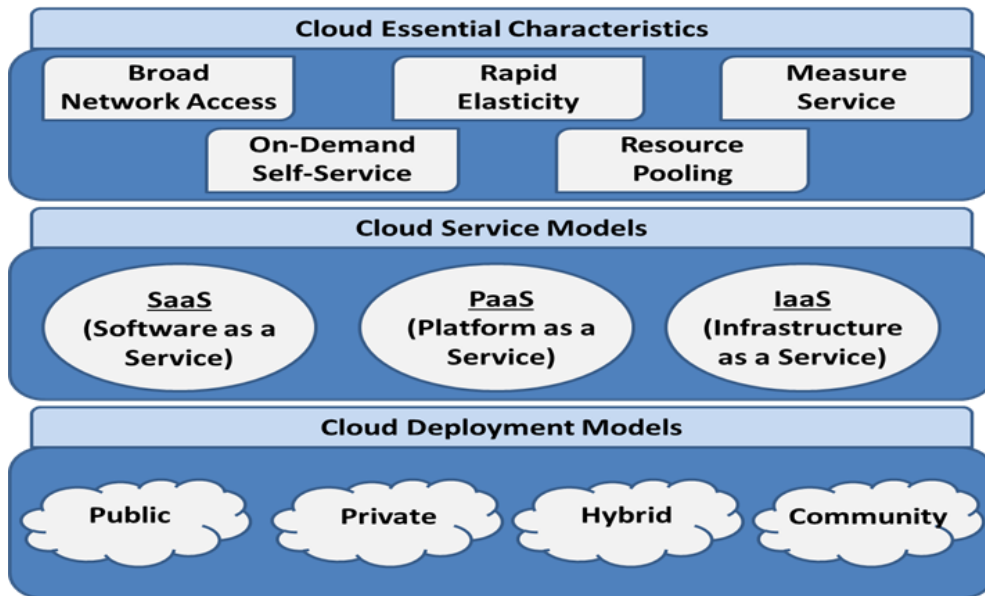


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

*On-demand self-service*

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

*Broad network access*

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

*Resource pooling*

The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction

(e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

### *Rapid elasticity*

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

### *Measured service*

Cloud systems automatically control and optimize resource use by leveraging a metering capability\* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

*\* Typically this is done on a pay-per-use or charge-per-use basis.*

## Deployment Models:

### *Private cloud*

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

### *Community cloud*

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

### *Public cloud*

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

### *Hybrid cloud*

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

## Service Models:

### *Software as a Service (SaaS)*

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure\*.

*\* A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as “Software deployed as a hosted service and accessed over the Internet.”

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

### *Platform as a Service (PaaS)*

This model provides the consumer the capability to deploy consumer-created or acquired applications\* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

*\* This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

### *Infrastructure as a Service (IaaS)*

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select

networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

### **Key Security and Privacy Issues:**

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—*at the extreme, displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

### Governance

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

## Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

### *Law and Regulations*

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

### *Data Location*

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

### *Electronic Discovery*

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.



## Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

### *Insider Access*

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

### *Data Ownership*

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

### *Visibility*

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

### *Ancillary Data*

While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

### *Risk Management*

Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

### Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

### Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

### Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost

benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

### Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

### *Value Concentration*

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

### *Data Isolation*

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

### *Data Sanitization*

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

## *Encryption*

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.
- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.
- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

## Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

## Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

### *Data Availability*

The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

### *Incident Analysis and Resolution*

An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

## **General Recommendations:**

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

**Table 1: Security and Privacy Issue Areas and Recommendations**

Areas	Recommendations
Governance	<ul style="list-style-type: none"> <li>Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.</li> <li>Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.</li> </ul>
Compliance	<ul style="list-style-type: none"> <li>Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements.</li> <li>Review and assess the cloud provider’s offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements.</li> <li>Ensure that the cloud provider’s electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.</li> </ul>
Trust	<ul style="list-style-type: none"> <li>Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time.</li> <li>Establish clear, exclusive ownership rights over data.</li> <li>Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system.</li> <li>Continuously monitor the security state of the information system to support on-going risk management decisions.</li> </ul>
Architecture	<ul style="list-style-type: none"> <li>Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.</li> </ul>
Identity and Access Management	<ul style="list-style-type: none"> <li>Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.</li> </ul>
Software Isolation	<ul style="list-style-type: none"> <li>Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.</li> </ul>
Data Protection	<ul style="list-style-type: none"> <li>Evaluate the suitability of the cloud provider’s data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.</li> </ul>

- Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.
- Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.

---

Availability

- Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements.
- Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstated in a timely and organized manner.

---

Incident Response

- Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.
  - Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.
  - Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.
-

## **G.4 Mobile Appendix**

### **Mobile Appendix**

#### **Introduction**

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolution of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

#### **Mobile Device Risk Scenarios**

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and 'Pocket sized' devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.



## *Device Categories*

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

### *Laptop devices*

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a ‘traditional’, full-featured operating system (e.g. Windows or a Linux variant). Also included in this category are ‘tablet’ type full-featured computers running a traditional full-featured operating system but without an attached keyboard. The main defining factor is the use of a full-featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user’s body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

### *Tablet devices*

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited-feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited-feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can

function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. ‘always on cellular’ vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

### *Pocket devices/Handheld devices*

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or ‘holster’ attached to the body. The bulk of this category will be cellular ‘smartphones’ with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full-feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

### *Device Connectivity*

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes ‘on demand’ cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either through the operating system or a third-party mobile device management (MDM) system may be

able to significantly control and define which particular connectivity risks may be associated with a particular device.

#### *Cellular Network Only (always on)*

Cellular network connectivity is characterized by ‘always on’ network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with ‘always on’ cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as ‘always on’ or ‘on demand’. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain ‘airplane’ mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other ‘eavesdropping’ devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a ‘personal firewall’ if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full-featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an ‘always on’ cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

#### *WiFi only (includes ‘on-demand’ cellular)*

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or ‘connected’ to the cellular network. They connect to the network or internet through WiFi ‘hotspots’ or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over ‘public’ WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with ‘on-demand’ cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking (‘bricking’) or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full-featured laptops but may not be available for limited-feature mobile operating systems.

#### *Cellular (always on) + WiFi Network*

This is a hybrid scenario that has become typical with most ‘smartphones’. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

#### **Incident Handling (CJIS Security Policy Section 5.3)**

Additional or enhanced incident reporting and handling procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and

response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

### ***Loss of device Control***

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: “Is it reasonable to assume CJI could be accessed”) as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a ‘momentary’ loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while ‘minimal’ durations might include a few minutes of time and ‘extended’ periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

### ***Total Loss of device***

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out

of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

### ***Potential device Compromise (software/application)***

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

### **Audit and Accountability (CJIS Security Policy Section 5.4)**

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device will be necessary to ensure appropriate levels of auditing exist.

#### ***Auditable Events (reference 5.4.1)***

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and

consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

### ***Audit Event Collection***

Mobile devices without an ‘always-on’ cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in place for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

### **Access Control (CJIS Policy Section 5.5)**

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in ‘general’ purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

### ***Device Control levels and access.***

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) may bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

### ***Embedded passwords/login tied to device PIN.***

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a 'corporate' email application may independently encrypt the data associated with the application and require a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

### ***Access requirement specification***

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

### ***Special Login attempt limit***

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.



### *Login failure actions*

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

### ***System use Notification (CJIS Policy reference 5.5.4)***

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

### ***Session Lock (CJIS Policy reference 5.5.5)***

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

### ***Device WiFi Policy***

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

#### ***Hotspot capability***

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

#### ***Connection to public hotspots***

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

#### ***Cellular Service abroad***

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a 'trusted' entity by the device.

Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

### ***Bluetooth***

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

### ***Voice/Voice over IP (VoIP)***

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

### ***Chat/Text***

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

### *Administrative Access*

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from ‘general user’ access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of ‘routine’ device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

### *Rooting/Jailbreaking*

‘Rooting’ (Android OS) or ‘Jailbreaking’ (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of ‘traditional’ anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a ‘stock’ Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with ‘rooting’ and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate ‘secure’ versions of the Apple iOS and it is unlikely they will be developed.

### **Identity and Authentication**

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

#### ***Utilizing Unique device Identification***

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

### *Certificate Use*

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to ‘unlock’ the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

### *Certificate Protections*

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

### ***Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)***

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

### **Configuration Management**

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full-featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

### ***Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)***

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of

unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

### ***Device Backups/Images***

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

### ***Bring Your Own device (BYOD) employment***

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

### ***Configurations and tests***

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

## **Media Protection**

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the ‘internal’ storage of the device, the Android OS does not provide secure separation of data stores on ‘external’ storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific ‘external’ media protection requirements which may actually include built-in media or storage.

### ***Protection of device connected media***

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

### ***Encryption for device media***

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

## **Physical Protection**

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

### ***Device Tracking/Recovery***

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via ‘always-on’ cellular data connections and the devices built-in GPS. Device tracking with WiFi only or ‘on-demand’ cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered



when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

### ***Devices utilizing unique device identification/certificates***

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

### **System Integrity (CJIS Policy Section 5.10)**

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

### ***Patching/Updates***

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without ‘always-on’ cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

### ***Malicious code protection/Restriction of installed applications and application permissions***

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing

other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a matter analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full-featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

**TECHNOLOGY NOTE:** In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed by means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied

installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

**WARNING:** Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

### ***Firewall/IDS capability***

Traditional device or “personal” firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating system as long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

### ***Spam Protection***

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

### ***Periodic system integrity checks***

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

## **G.5 Administrator Accounts for Least Privilege and Separation of Duties**

### Administrator Accounts for Least Privilege and Separation of Duties

#### **PURPOSE:**

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

#### **ATTRIBUTION:**

- SANS, “The Critical Security Controls for Effective Cyber Defense”, version 5.0
- NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations”, Revision 4 dated April 2013
- NIST SP 800-12, “An Introduction to Computer Security: The NIST Handbook” dated October 1995
- CNSSI-4009, “National Information Assurance (IA) Glossary”, dated April 2010

#### **DEFINITIONS:**

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

#### **SUMMARY:**

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all

required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

## **USER ACCESS AND ACCOUNT MANAGEMENT:**

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user's role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account

management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

## **THREATS:**

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

### *Phishing Attacks*

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user's account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

### *Password Brute Force Guessing / Cracking*

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that

are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

## **MITIGATION:**

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g. firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

## **NIST CONSIDERATIONS FOR LEAST PRIVILEGE:**

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of



the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

### **AC-6 Least Privilege**

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

#### Control Enhancements:

#### **(1) LEAST PRIVILEGE / AUTHORIZE ACCESS TO SECURITY FUNCTIONS**

**The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information].**

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

#### Control Enhancements:

#### **(2) LEAST PRIVILEGE / NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS**

**The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.**

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

### **(3) LEAST PRIVILEGE / NETWORK ACCESS TO PRIVILEGED COMMANDS**

**The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.**

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

### **(4) LEAST PRIVILEGE / SEPARATE PROCESSING DOMAINS**

**The information system provides separate processing domains to enable finer-grained allocation of user privileges.**

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

### **(5) LEAST PRIVILEGE / PRIVILEGED ACCOUNTS**

**The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].**

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

**(6) LEAST PRIVILEGE / PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS**

**The organization prohibits privileged access to the information system by non-organizational users.**

Supplemental Guidance: Related control: IA-8.

**(7) LEAST PRIVILEGE / REVIEW OF USER PRIVILEGES**

**The organization:**

**(a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and**

**(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.**

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

**(8) LEAST PRIVILEGE / PRIVILEGE LEVELS FOR CODE EXECUTION**

**The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.**

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such

applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

**(9) LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS**

**The information system audits the execution of privileged functions.**

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

**(10) LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS**

**The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.**

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-6 (1) (2) (5) (9) (10)	HIGH AC-6 (1) (2) (3) (5) (9) (10)
----	------------------	-------------------------------	------------------------------------

**SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS)  
CONSIDERATION FOR LEAST PRIVILEGE:**

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the “20 Critical Security Controls for Effective Cyber Defense”. This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled “Controlled Use of Administrative Privileges”. SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

### **Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges**

*The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

<b>ID #</b>	<b>Description</b>	<b>Category</b>
CSC 12--1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	<i>Quick win (One of the “First Five”)</i>
CSC 12--2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive	<i>Quick win</i>
CSC 12--3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	<i>Quick win</i>

CSC 12--4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration--level accounts.	<i>Quick win</i>
CSC 12--5	Ensure that all service accounts have long and difficult--- to--- guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	<i>Quick win</i>
CSC 12--6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800--132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super---user privileges.	<i>Quick win</i>
CSC 12--7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e---mail, composing documents, or surfing the Internet. Web browsers and e---mail clients especially must be configured to never run as administrator.	<i>Quick win</i>
CSC 12--8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non---administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows “administrator” or UNIX “root” accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	<i>Quick win</i>
CSC 12--9	Configure operating systems so that passwords cannot be re--- used within a timeframe of six months.	<i>Quick win</i>
CSC 12--10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators’ group, or when a new local administrator account is added on a system.	<i>Visibility/ Attribution</i>
CSC 12--11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	<i>Visibility/ Attribution</i>

CSC 12--12	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	<i>Configuration/ Hygiene</i>
CSC 12--13 (NEW)	When using certificates to enable multi-factor certificate-based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	<i>Configuration/ Hygiene</i>
CSC 12--14	Block access to a machine (either remotely or locally) for administrator-level accounts. Instead, administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	<i>Configuration/ Hygiene</i>

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

## **SEPARATION OF DUTIES:**

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection

against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

### **THREATS:**

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g. a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

### **MITIGATION:**

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.



Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

## **NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:**

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements but it is significant in protecting the integrity of an information system.

### **AC-5 Separation of Duties**

Control: The organization:

- a. Separates [*Assignment: organization-defined duties of individuals*];
- b. Documents separation of duties of individuals; and
- c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5
----	------------------	----------	-----------

## G.6 Encryption

### Encryption

#### **Purpose:**

This paper was created to provide assistance and guidance on encryption types, methods, and to provide general best practices in the implementation of encryption.

#### **Attribution:**

- FIPS 140 – 2, Security Requirements for Cryptographic Modules (May 2001)
- FIPS 197, Advanced Encryption Standard (Nov 2001)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information among Security Systems
- CJIS Security Policy

#### **Definitions and Terms:**

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Asymmetric Encryption – A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Symmetric Encryption – A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

Hybrid encryption – A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Authorized User/Personnel - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

### **Summary:**

CJIS Security Policy encryption requirements are intended to provide protection of the sensitive data that is criminal justice information (CJI). The primary goal of encrypting CJI is to prevent unauthorized access to this sensitive data. Encryption is a great tool that can be applied to accomplish this protection and ensure compliance with the vast majority of the CJI requirements. CJIS Security Policy Section 5.10.1.2 details when encryption is required and provides information on the exceptions to the encryption requirement.

### **Achieving CJIS Security Policy Compliance:**

To determine when encryption is required one must first read and understand CJIS Security Policy Section 5.9.1 Physically Secure Location. The reason for this is simple: encryption is not required while within a physically secure location. Conversely, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location encryption may be required. The exact standards to which the data would be required to meet are detailed along with any exceptions in CJIS Security Policy Section 5.10.1.2.

Additionally, both security awareness training and personnel security requirements can be affected by whether or not CJI is encrypted. Requirements surrounding these Policy areas is determined by answering the following question: Who has unescorted access to unencrypted CJI?

Unless personnel is escorted, security awareness training is required as correlated with the access level needed by personnel as identified in CJIS Security Policy Section 5.2. Similarly, fingerprint-based background checks as detailed in CJIS Security Policy Section 5.12 may be required on individuals to permit unescorted access to CJI.

The intent of all these requirements is to limit access to CJI to only authorized personnel. CJIS Security Policy Appendix A: Terms and Definitions defines authorized user/personnel as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

## **What is Encryption?**

Encryption is the process of encoding messages or information in such a manner that only people with the knowledge or means to decrypt the message can do so. But how does this work?

In an encryption process, legible data, referred to as plaintext, is encrypted by applying a cipher (otherwise known as an encryption algorithm or crypto key) to the data. The data then becomes encrypted and is now referred to as ciphertext. The ciphertext is essentially unreadable until decrypted. The decryption process requires the process of applying the same algorithm (crypto key) to encrypt the data in an inverse manner to convert the data back into plaintext.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Encryption has been used throughout history to send “secrets” securely by some form of obfuscation to a recipient. Businesses and enterprises use encryption to protect corporate secrets and sensitive employee data, such as payroll information and personally identifiable information (PII). Governments secure classified information with encryption. Additionally, individuals may use encryption to protect personal information, such as credit card data, banking information, and passwords to guard against things like identity theft.

It should be known that encryption may not always prevent the interception of data. If the stolen data is encrypted, though, it would be extremely difficult for any of the data to be decrypted without having the decryption key. While it may be possible to decrypt the message without possessing the key, it does require large computational resources, great skill, and lots of time to accomplish such a task. Exercising encryption along with key management policies is one of the best security practices that can be put into place with regard to sensitive data security and protection.

## **Types of Encryption:**

### Symmetric Encryption

Symmetric encryption is also commonly known as secret key encryption. Symmetric encryption is a form of cryptography utilizing a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric encryption is most often used for data protection whether at rest or in transit, especially in bulk, due to the ease and speed with which the encryption can be implemented. The most common examples of symmetric algorithms are: AES and Triple-DES (3DES or TDEA).

How it works:

To encrypt and send a message to Jane, John does the following:

1. Generates a new symmetric key
2. Encrypts the message using this new symmetric key
3. Sends the message to Jane
4. Sends the encrypted symmetric key to Jane - out of band

To decrypt this ciphertext, Jane does the following:

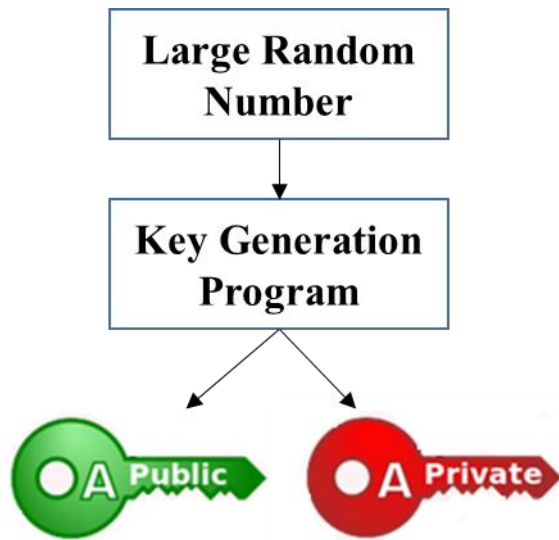
1. Receives the encrypted message
2. Receives the symmetric key
3. Uses the symmetric key to decrypt the message

### Asymmetric Encryption

Asymmetric encryption is also commonly known as public-key encryption. Asymmetric cryptography is cryptography in which a pair of keys, a public key and a private key, are used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Creating Key Pairs:

Asymmetric encryption requires the use of algorithms of great computational complexity to create the key pairs. This is accomplished by using a large, random number that an algorithm is applied to which generates a pair of keys for use as asymmetric key algorithms (as shown in Figure 1 below).



*Figure 1 – Asymmetric key pair generation*

Asymmetric encryption is most often used to encrypt a single message before transmission. The most common examples of asymmetric algorithms are: RSA and DSA.

How it works:

To encrypt and send a message to Jane, John does the following:

1. Obtains Jane's public key
2. Encrypts the message using Jane's public key
3. Sends the message to Jane

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Uses her private key to decrypt the message

### Advantages of Using Symmetric Encryption for Data Protection

Asymmetric encryption requires the use of algorithms with great computational complexity to create the key pairs, and therefore is not practical for large amounts of data. It is typically used for only for short messages. Also, asymmetric encryption must use a comparatively stronger key than symmetric key encryption to achieve the same level of protection as one key (public) will be published in the public directory for all to see.

Symmetric encryption is based on large, but simple algorithms which require less computation. Therefore, is much faster to create and use keys. This allows the same key to be used to encrypt and decrypt the message. So, data can be encrypted in real time. The (shared) key is sent to the recipient out of band so that it can be used to decrypt the data.

For the reasons stated above, symmetric key encryption is the preferred choice by both industry and government alike to encrypt large amounts of data (bulk encryption) simply due to the ease and real time encryption capabilities as detailed above. Additionally, a new key can be generated for every session, message transaction, etc., as desired. This means a sender won't have to use one key (public) to encrypt a message and have the recipient use another key (private) to decrypt the message.

### Hybrid Encryption

Hybrid encryption solution exist where both asymmetric encryption and symmetric encryption keys are used to create what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hybrid solutions are most often used by Internet browsers to protect data in transit. The most common examples of hybrid encryption are: TLS/SSL, PGP, IPSEC, and S/MIME.

How it works:

To encrypt a message to Jane in a hybrid cryptosystem, John does the following:

1. Obtains Jane's public key
2. Generates a new symmetric key
3. Encrypts the message using this new symmetric key
4. Encrypts the symmetric key using Jane's public key
5. Sends the message to Jane

To decrypt this hybrid cipher text, Jane does the following:

1. Receives the encrypted message
2. Receives the encrypted symmetric key
3. Uses her private key to decrypt the symmetric key
4. Uses the symmetric key to decrypt the message

Explaining Cipher Suites:

A cipher suite is a set of cryptographic algorithms used for the following:

- Protect information required to create shared keys (key exchange)
- Encrypt messages exchanged between clients and servers (bulk encryption)
- Generate message hashes and signatures to ensure the integrity of a message (message authentication)

Examples of Transport Layer Security (TLS) 1.2 Cipher Suites:

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

A cipher suite specifies one algorithm for each of the above tasks. For example, the TLS\_RSA\_WITH\_AES\_128\_SHA256 cipher suite is used for TLS. The suite uses the RSA asymmetric algorithm for key exchange, AES with a 128-bit key for bulk data encryption, and SHA256 for message authentication.

Symmetric and Asymmetric Key Strength Comparison:

<u>Symmetric</u>		<u>Asymmetric</u>		
<u>Bits of security</u>	<u>Symmetric key algorithms</u>	<u>Finite-Field Cryptography (FFC)</u> <u>(e.g., DSA, D-H)</u> <u>Bits of security</u>	<u>Integer-Factorization Cryptography (IFC)</u> <u>(e.g., RSA)</u> <u>Bits of security</u>	<u>Elliptic-Curve Cryptography (ECC)</u> <u>(e.g., ECDSA)</u> <u>Bits of security</u>
<u>80</u>	<u>2TDEA18</u>	<u>Public key = 1024</u> <u>Private key = 160</u>	<u>Key size = 1024</u>	<u>Key size = 160-223</u>
<u>112</u>	<u>3TDEA</u>	<u>Public key = 2048</u> <u>Private key = 224</u>	<u>Key size = 2048</u>	<u>Key size = 224-255</u>
<u>128</u>	<u>AES-128</u>	<u>Public Key = 3072</u> <u>Private key = 256</u>	<u>Key size = 3072</u>	<u>Key size = 256-383</u>
<u>192</u>	<u>AES-192</u>	<u>Public key = 7680</u> <u>Private key = 384</u>	<u>Key size = 7680</u>	<u>Key size = 384-511</u>
<u>256</u>	<u>AES-256</u>	<u>Public key = 15360</u> <u>Private key = 512</u>	<u>Key size = 15360</u>	<u>Key size = 512+</u>

Figure 2 - Symmetric and asymmetric key strength comparison



As you can see in the chart provided above, the equivalent key strengths between symmetric and asymmetric key strengths do not necessarily correlate. There is a reason for this. As stated previously, asymmetric algorithms must use a comparatively stronger key than symmetric key encryption to achieve the same strength. The simplest explanation for this is because one of the keys is published to the public directory and can constantly be attacked by anyone with access to the directory. Therefore, the public key must be made of such strength that it can resist getting compromised while made public.

## **Federal Information Processing Standard (FIPS) 140-2 Explained**

### Origin of FIPS 140-2

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 to supersede the original FIPS 140-1. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) is a standard developed and recommended (often mandated) for use in federal-government-operated IT systems by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS 140-2 specifies the security requirements a cryptographic module must meet when utilized within a security system protecting sensitive information within information systems (computer and telecommunication systems). FIPS 140-2 specifies which encryption algorithms can be used and how encryption keys are to be generated and managed.

How does a product get certified?

Vendors of cryptographic modules can have their products tested by independent, accredited Cryptographic and Security Testing (CST) laboratories. The CST laboratories use the Derived Test

Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards in a variety of implementations. The result of these tests are reported to NIST's Computer Security Division (CSD) and CSEC who jointly serve as the Validation Authorities for the program. These results are then reviewed and certificates would be issued if the results are determined to be acceptable.

What is the difference between being FIPS 140-2 compliant and being FIPS 140-2 certified?

It is common theme to discover a product is “FIPS compliant.” What does this mean, though? The difference between compliance and certification is not subtle. Certification requires a vast testing, verification, and validation process be performed by a CST laboratory as described in the previous section. Compliance is merely a claim stating the implementation of an encryption solution is done in accordance with the security policy related to the FIPS certification. Any claim of compliance would need to be validated and the corresponding certificate number would have to be known.

NIST has addressed related claims as shown below in their Frequently Asked Questions for the Cryptographic Module Validation Program:

A vendor makes the following claims of conformance to FIPS 140-2. Are they acceptable?

- The module has been designed for compliance to FIPS 140-2. <NO>
- Module has been pre-validated and is on the CMVP pre-validation list. <NO>
- The module will be submitted for testing. <NO>
- The module has been independently reviewed and tested to comply with FIPS 140-2. <NO>
- The module meets all the requirements of FIPS 140-2. <NO>
- The module implements FIPS Approved algorithms; including having algorithm certificates. <NO>
- The module follows the guidelines detailed in FIPS 140-2. <NO>
- The module has been validated and has received Certificate #XXXX. <YES>

A cryptographic module does not meet the requirements or conform to the FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

To read more FAQs from NIST on FIPS certification, use the following NIST website link:  
<http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf>

Where can I learn more about FIPS 140-2?

For more information about the FIPS 140-2 standard, go to the following NIST website:  
<http://csrc.nist.gov/cryptval/140-2.htm>

### **General Recommendations:**

Encryption key management control is of paramount importance! Agencies should develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys. After all, encryption keys should not be accessible by just anyone. An encryption key management control process should ensure only authorized users have access to encryption keys. Key management is a best security practice and helps to ensure the confidentiality and integrity of CJI data and enforces key access control.

The CJIS Security Policy is a “living” document under constant review and receiving regular updates through the Advisory Policy Board (APB) process. Agencies need to always keep up to date on the latest requirements. These requirements can be found in CJIS Security Policy Section 5.10.1.2. Please contact the CJIS ISO Program anytime to address any questions or concerns about CJIS Security Policy requirements, the current APB status of CJIS Security Policy requirements, or if seeking general information or guidance.

## G.7 Incident Response

### Incident Response

#### Introduction

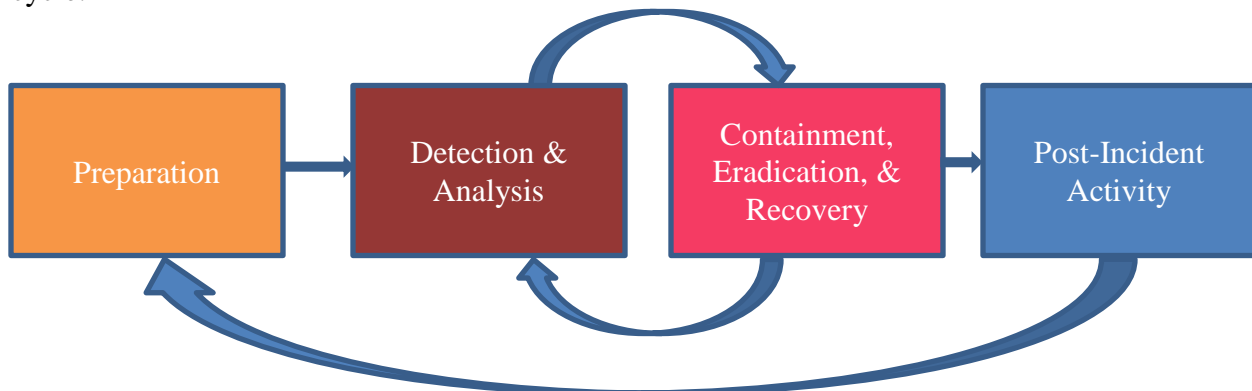
---

Information technology (IT) security incident response is an important and critical component of information technology programs. Performing incident response effectively can be a complex undertaking – for that reason, establishing a successful incident response capability requires planning and resources. Everyone in an organization must be aware of IT security risks, threats, and actions to take in situations where an actual IT security incident has occurred. Even the best-secured and controlled environments can experience these security risks, threats, events, and incidents. This document provides guidelines for appropriate response to IT security incidents, and are independent of specific hardware platforms, operating systems, protocols, or applications.

The following example incidents are used to highlight appropriate actions during each phase:

- Malicious code execution
- Ransomware execution
- Denial of service attack
- Social Engineering
- Phishing

NIST Special Publication 800-61 rev. 2 outlines the “Incident Response Life Cycle” as a collection of phases – distinct sets of activities that will assist in the handling of a computer security incident, from start to finish. The following diagram explains the process flow of the incident response life cycle:



## Preparation

---

The initial phase of the incident response life cycle, “Preparation”, involves establishing and training an incident response team, and acquiring the necessary tools and resources. A computer security incident may not have happened at this phase, but it is important to utilize all available knowledge and security measures to obtain the best posture for responding to potential future incidents. One of the most important preparation steps involves the collection, storage, and accessibility of event data and telemetry from hardware and software resources such as firewall logs, application logs, operating system logs, and other valuable sources of situational data, as well as the output of products that perform analysis on such data. Preventive measures to mitigate or eliminate future incidents are deployed during this phase, using industry best practices, data obtained from research and intelligence sources, and lessons learned from past incidents.

It is also imperative to prepare a list of contact information or notification methodologies to employ when an incident occurs, as well as notification and communication strategies within the team, with stakeholders, and with upper management and potentially other criminal justice and non-criminal justice agencies. This will help ensure that when incidents arise, the proper personnel and organizations are notified and kept informed of the circumstances regarding the incident.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Preparation phase can be given:

### **Malicious code execution**

Preparation for incidents involving malicious code execution should initially involve user awareness of sources of malicious code. There are many potential sources of malicious code, such as web pages, emails, and removable media. The utilization and deployment of effective antivirus software, integrity-monitoring software, and intrusion detection and prevention software are effective measures to take to prepare for incidents involving malicious code execution.

### **Ransomware execution**

Preparation phase activities for incidents involving ransomware execution are much the same as activities for malicious code execution, as ransomware is a specialized form of malware that encrypts potentially important or critical files, with the intention of coercing a victim to pay for a decryption key. Implementing a robust offline backup solution for these types of files is an important preparative action to take regarding the execution of ransomware. This will ensure that when ransomware attacks do happen, the mission impact is as minimal as possible and very little or no data is lost.

## **Denial of service attack**

Denial of service attacks are given attention in the preparation phase. Defensive responses to denial of service attacks typically involve the use of a combination of attack detection and traffic classification and response tools, aiming to block traffic identified as abusive denial of service activity. Deploying solutions such as IDS/IPS devices and software, network hardware with rate-limiting capabilities (routers, switches, and firewalls), and upstream filtering devices at the system perimeter can mitigate for denial of service attacks.

## **Social Engineering**

Preparation for social engineering attacks starts with user awareness training. Understanding and identifying attempts to obtain information in an unauthorized manner is crucial to thwarting these types of scenarios. Social engineering is the art of manipulating people to obtain information they may not be authorized to handle. Training and routinely testing users on potential social engineering scenarios and tactics, and providing training regarding appropriate responses to requests involving personal or otherwise sensitive information (for example, passwords or criminal justice information), is an effective way to ensure social engineering attacks never traverse past the preparation phase of the incident response life cycle.

## **Phishing**

Like social engineering, preparation for phishing attacks is imperative. Phishing is a social engineering technique attackers employ to deceive users, in a fraudulent attempt to obtain sensitive information, or to gain unauthorized access to systems. Phishing is extremely widespread, and attackers disguising fraudulent scenarios in electronic communication such as email and instant messages are the most common. User awareness of these types of tactics is paramount to prepare for phishing attacks and schemes.

## **Detection and Analysis**

---

The detection and analysis phase begins when a security incident has occurred. To understand when this phase begins, there must be a capability for an intelligent determination of circumstances constituting a security incident. Specialized knowledge and highly trained personnel are necessary for this step to be effective. Many organizations employ teams of personnel who are specifically trained to handle the intricacies of the incident response life cycle. The determination of a security incident can arise from one or several circumstances simultaneously – for example:

- Trained personnel manually reviewing collected event data for evidence of compromise
- Software applications analyzing events, trends, and patterns of behavior
- The observation of suspicious or anomalous activity on a computer system

The goals of this phase are:

- To detect whether a security incident occurred
- To determine the vector (i.e., method) of attack
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident
- To obtain or create intelligence products regarding attack vectors and methodologies, especially when dealing with malicious code

Prioritization of incidents is also an important decision point in the incident response life cycle, as the circumstances regarding an incident can bring the situation to a critical level. There are three major impacts to consider when addressing priority of incidents:

- **Functional Impact:** the impact to business functionality
- **Information Impact:** the impact to confidentiality, integrity, and/or availability of criminal justice information
- **Recoverability:** the amount of time and resources that must be spent on recovering from an incident

Documentation regarding an incident should be thorough and applicable to the incident. This can be crucial in incidents that may lead to legal prosecution, as well as being invaluable to efficiently document, track, handle, manage, and resolve one or more incidents at the same time.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Detection and Analysis phase are given:

### **Malicious code execution**

Detection of malicious code execution is often a primary job of host-based antivirus software. Having a capable and up-to-date antivirus solution installed on a system can detect known malicious code, as well as detect potentially malicious behaviors. The delivery of malicious code to a system can be detected by network traffic analysis and protection tools and hardware. Additionally, some malicious code may produce network traffic that is indicative of successful execution, exploitation, and/or compromise of a system. Solutions such as intrusion detection/prevention systems, Security Information and Event Management (SIEM) tools, and file integrity monitoring software can provide the necessary level of fidelity to make a determination of malicious code execution.

Knowing if or when a system is infected is not always immediately evident. Security controls may have been bypassed or even disabled by the malicious code. However, systems infected by malicious code or software (i.e. malware) can exhibit several indicators. These indicators include, but are not limited to:

Unexpected pop-up windows

- Slow start up and/or slow performance
- Suspicious hard drive activity including an unexpected lack of storage space
- Missing files
- Crashes and/or error messages
- Unexplained network activity
- Hijacked email

Analysis of malicious code can be performed in several ways. Static analysis of malicious code can be performed to determine the capabilities of the malicious code and generate actionable intelligence. Dynamic analysis of malicious code can be used to observe how the malicious code interacts with the system and what actions it performs and can often more rapidly determine the capabilities of malicious code. Both static and dynamic analysis can be performed manually, as well as in an automated fashion. Trained specialized personnel are crucial to the analysis of malicious code.

### **Ransomware execution**

The detection of ransomware is identical to the detection of malicious code. Ransomware is specialized malicious code that encrypts potentially valuable files, generally with the intent to coerce a victim to pay a ransom for the possibility of the decryption of those files. Host-based antivirus solutions can also detect these threats, and network traffic analysis and protection tools and hardware can be used to prevent the successful execution of ransomware. SIEM tools and file integrity monitoring software can also detect the execution of ransomware.

Analysis of ransomware is identical to the analysis of malicious code, and the same intelligence can be determined in the same fashion as with the analysis of malicious code. The most obvious sign that ransomware has affected a system is the existence of encrypted files, the disappearance of certain types of files, and/or the presence of “ransom notes” on the system, which contain instructions for payment to obtain a decryption key, which may or may not be legitimate.

### **Denial of service attack**

Denial of service (DoS) attacks are often detected at the perimeter of an organization but can also be detected within the organization as well. Often, from a user’s perspective, the signs of a DoS attack appear to be network performance or administrative maintenance related issues such as slow or broken network connections or down websites. Additionally, an administrator may notice ping time outs, event logs overflowing or alerts from network monitoring systems as issues that may identify a DoS attack. Intrusion detection and prevention software and platforms can detect denial of service attacks, as well as some network monitoring hardware and appliances, such as web application filters, routers,



firewalls, and switches. Devices targeted by denial of service attacks can also detect the attacks in some instances, if they have the capabilities to determine explicit attack activity versus normal network traffic.

Analysis of denial of service attacks include the determination of the source traffic, the protocols used to generate the traffic, the service(s) targeted by the attack, and the potential impacts of the attack. Network monitoring devices can often provide these types of data, with the exception of potential impacts of denial of service attacks on systems.

## **Social Engineering**

Detection of social engineering attacks is primarily based on the situational awareness of the individual targeted by social engineering. Given that social engineering is a broad topic that can involve the manipulation and exploitation of people in control of an information system, user awareness of social engineering attempts is crucial. If the target has security awareness training in detecting attempts to gain information or access in an unapproved manner, social engineering is easier to detect.

Analysis of social engineering attacks will generally rely on the recollection abilities of or documentation taken by the targets of the attack. Social engineering may not occur on an information system and may be completely carried out in-person. If the target can recollect or produce documentation regarding the social engineering attempt, the motivation and desired access can potentially be determined. For successful social engineering attempts, recollection and documentation of the attempt is crucial to determining the level of unauthorized access that was obtained.

## **Phishing**

Detection of phishing attacks generally will first occur at an organization's email point of presence. Some organizations still run their own email servers, and many have migrated to cloud solutions. Having an on-premise email server or server farm or cluster will require additional functionality to detect phishing attempts. For example, the header content of the email will need to be read, as well as the content inside the body of the email, to check for potentially malicious content and potentially falsified data that may indicate a phishing email. Many cloud email providers have built this capability into their email solutions, but it is still possible for users to receive phishing emails, as attacker tactics and capabilities evolve daily. The most effective detection of phishing comes from heightened situational awareness of potential attacks. Validating the source of the email can uncover potential phishing attempts.

Analysis of phishing attacks involves examination of email headers, as well as contents of the body of the email. The body of the email may contain malicious content, attachments, or links to suspicious or malicious content. Manual or automated analysis activities can be

performed on the email content. Analysis of these elements should be performed by trained specialized personnel to generate intelligence and aid with the determination of indicators of compromise.

## Containment, Eradication, and Recovery

---

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. Often, this requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels can be invaluable to the implementation of containment activities. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication efforts for a computer security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents involve restoration of affected systems to normal operation. This may include actions like restoring systems from backups, rebuilding systems from an agency-approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Compromised hosts are often attacked during these phases, as attackers try to regain their foothold on compromised systems or systems on the same network or others in the logical vicinity.

### **Malicious code execution**

Containment activities for malicious code execution involve the logical or physical isolation of the host from the attacker's control and from any mission services or systems that would be impacted by the compromised host. This may include putting the host in a restricted VLAN, using firewalls to block traffic, disconnecting it from the network completely, shutting it down, or disabling functionality. Exercise caution as malicious code may have capabilities to take further actions on a host in case communications with a command and control server are severed. It is important to understand the capabilities of the malicious code before taking containment actions.

Eradication activities include the removal of malicious code from the system. This may be as simple as removing files, configuration rules, accounts, and other persistent items that the malicious code utilizes to function and maintain a presence on the system. This phase

also involves the discovery and removal of indicators of compromise on other systems, if applicable. It is imperative to remediate vulnerabilities that may have been exploited during eradication as well.

Recovery from malicious code execution generally is similar across many environments. Rebuilding the system from a clean baseline or restoring files from backup are typical activities that help restore the functionality of the system to continue the mission. Changing system passwords, installing patches, implementing tighter network access control, and ensuring appropriate levels of logging fidelity of the information system are integral parts of the recovery process.

### **Ransomware execution**

Containment for ransomware execution should be as swift and immediate as possible, as ransomware can execute and spread to accessible media at a rapid pace. Considering files are being encrypted or have already been encrypted, immediate action should be taken to logically or physically isolate the system by disconnecting network connectivity. It is up to the system owner whether to take the risk in powering off the system, as valuable forensic artifacts may be destroyed in the process, but it will halt the execution of the ransomware and protect potentially valuable files. Please note that containment of active ransomware execution is one of the only circumstances where measures such as immediate shutdown are recommended.

Eradication of ransomware does not need to occur in most circumstances, as the entire goal of ransomware is to encrypt files and leave “recovery” instructions to extort victims. The vast majority of ransomware will delete itself once encryption of files is complete, but it is possible that some ransomware is persistent and can remain on the system. If this is the case, analysis should be performed on the ransomware to determine its capabilities, and eradication activities will proceed in an identical fashion to malicious code execution eradication activities.

Recovery from ransomware execution involves restoring encrypted files from backup and may involve the rebuilding of an entire system depending on the extent of the encryption from the ransomware. If a robust offline backup solution for hosts is not present or not utilized on a regular basis, the loss of potentially valuable data may be incredibly costly in several areas to repair, to include man-hours, revenue, and business products, data, and intelligence.

### **Denial of service attack**

Containment of denial of service attacks involve the modification of access control where the attack is occurring. For example, if a web or application server is experiencing a denial of service attack, the system itself, as well as network monitoring devices, should be

examined to determine the source of the attack traffic. Once the source of the traffic is identified, modifications to access controls or rate-limiting features such as firewall access controls lists (ACLs) and web application filters can be employed to block the traffic. Care must be taken to determine if the observed traffic is actually intentional malicious denial of service traffic, versus heavy legitimate network traffic. Implementing access control mechanisms or rate-limiting features may negatively affect the mission of the system. It is also important to note that manual containment in this fashion may not be entirely effective, as attackers can circumvent the ACL by changing the attacking IP address, protocol, or other attribute of the connection.

Eradication is not necessarily applicable in denial of service scenarios, unless a vulnerability or misconfiguration is being exploited to cause the denial of service condition. If this is the case, take steps to remediate the vulnerability or misconfiguration.

Recovery actions depend on the available resources of the information system. For example, on-premise load balancers can be used to distribute the traffic, whether legitimate or malicious, to other less-burdened systems. Many cloud providers and content delivery networks also have denial of service mitigation capabilities. It may also be prudent to increase the resources (memory, processing capacity) of internet-facing systems so that they can handle larger amounts of traffic simultaneously.

## **Social Engineering**

Containment regarding social engineering attacks is dependent upon the information or access that was provided to the attacker. For example, if an attacker gained access to an account on a system following a social engineering attempt, the account should be administratively disabled and all sources of event data regarding that account should be immediately collected. If sensitive data was divulged to the attacker, the impact of the exposure of that data should be examined and mitigating activity should be initiated to determine or reduce the damage of the spread of the information.

Eradication regarding social engineering attacks also depends on the information or access provided to the attacker. Removing or limiting the provided access is a pertinent eradication action. If the information provided is a credential to a system, disable and remove the credential from the system. Eradication may also involve the physical detainment or removal of personnel from a site.

Recovery actions for social engineering attacks are dependent on the information or access provided to the attacker. Additionally, security awareness training is an appropriate recovery action to ensure staff understands the threats of social engineering.

## Phishing

Containment of phishing activity is tied very closely to the identification and analysis of the phishing activity. Understanding the tactics of the phishing attacker is paramount to deploying containment activities. Activities include, but are not limited to, administratively blocking sender email addresses and IPs, blocking potential malicious content in email via a web proxy, communicating with potential recipients, and implementation of email content or hyperlink blacklisting if possible. Phishing attacks can also include attempts to have users execute malicious code on systems, where containment activities regarding malicious code will be applicable.

Eradication of phishing attacks include the administrative removal of the emails from email systems, as well as eradication actions for malicious code if applicable.

Recovery from phishing attacks can include:

- Implementation and enforcement of the Domain Keys Identified Mail (DKIM) email authentication method, which can mitigate the possibility that attackers can send spoofed email
- Implementation and enforcement of Sender Policy Framework (SPF) to control and stop sender forgeries
- Implementation and enforcement of Domain-based Message Authentication, Reporting, and Conformance (DMARC), which enables message senders to indicate that their messages are protected with SPF and/or DKIM

Additionally, if malicious code is present in the phishing attack, recovery actions regarding malicious code may be applicable.

## Post-Incident Activity

---

Post-incident activities occur after the detection, analysis, containment, eradication, and recovery from a computer security incident. Arguably one of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?

- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Smaller incidents, and those that are similar to others that have been well documented, do not necessarily need much focus in this phase of incident response. Larger and less-understood security incidents should be the focus of a comprehensive post-mortem evaluation that outlines many of the items listed above and should include personnel that can have a direct impact on or are directly affected or responsible for the involved systems.

Post-incident activities such as these also help to serve as training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

### **Malicious code execution**

Post-incident activities for malicious code execution generally will follow similar patterns. A timeline of activity should have been prepared using digital forensic data collected during the detection and analysis phases of the incident. This timeline should include all affected systems and times of all activities and actions taken during the incident. Steps that victims and system administrators may have taken during the course of the incident, as well as in close proximity to the time range of the incident, are valuable items to document and discuss. Any deviation from organizational policy should be noted and taken as training items or assigned consequences in accordance with organizational policies. It may also be pertinent to ensure that appropriate information and intelligence sharing was performed during and after the incident occurred. Corrective actions that may have prevented the execution of malicious code, such as antivirus solutions, restrictions on where executables can run, tightened permissions, and script blockers for browsers, should be considered as a mitigation for the risks posed by malicious code threats. Web proxy blocks from information discovered during analysis can be utilized to ensure that malicious hosts are not contacted.

### **Ransomware execution**

Post-incident activities for ransomware execution include all the activities involved with malicious code execution, with the addition of ensuring the functionality of a robust offline backup solution. An offline backup solution ensures that backup data is kept inaccessible to ransomware threats and is available if ransomware is successfully executed. A functional and frequent (such as daily incremental and weekly full) backup process helps ensure that business continuity is maintained in the event of issues and incidents.

## **Denial of service attack**

Denial of service post-incident activities should include a timeline of traffic activities, as well as organizational responses to the attack traffic as well as the timeline of any business impacts and the damage associated with the impacts. Any attack precursors should be investigated and noted, and intelligence implemented to notify personnel and potentially take action as soon as attack traffic is observed. Impacts on affected systems should be noted, and a consensus should be reached on whether the systems should be upgraded or supplemented with load-balancing capabilities.

## **Social Engineering**

Post-incident activities for social engineering incidents should include a timeline that includes all applicable activities, such as points of contact, narratives from the parties involved, CCTV footage (if applicable), system and network log files, and physical access control logging data. If unauthorized access was obtained, the impact of the access should be assessed and mitigating factors should be identified for inclusion to reduce the risk of future incidents (such as multifactor authentication, physical locks, greater CCTV coverage, improved physical access control, etc.). Security awareness training should be imperative if policy was breached, and information or access was given to unauthorized parties.

## **Phishing**

Phishing post-incident activities should also include a timeline of actions taken since the phishing email was received, to include descriptions of the type of phishing campaign observed (malicious code, financial exploitation, credential harvesting, etc.), malicious attachments contained (if any), malicious or suspicious links in the body of emails, as well as narratives from recipients of the email and any potential victims, either self-reported or discovered through email, network, or host-based monitoring. If malicious code was included in the campaign, typical post-incident activities involving malicious code should be considered as well. Training opportunities can often arise from phishing attacks, whether successful or not, that can be valuable in giving employees better situational awareness regarding phishing.

The CJIS Security Policy requires each agency with access to CJI to establish operational incident handling procedures (i.e. a local policy). Gleaning from the requirements in Section 5.3 Incident Response, the local policy may include the following elements:

- Overall incident handling procedures. This section describes and identifies the processes used locally how the agency successfully prepares for, manages, and recovers from an incident. It includes sections on:
  - Preparation
  - Detection and Analysis
  - Containment

- Recovery
  - User response activities
- How the agency performs incident reporting. This section describes the process of notifying internal and external partners when an incident has occurred and how the incident is documented. It includes sections on:
  - Internal and external points of contact
  - Required tracking and reporting documents
  - Escalation procedures
- Incident management procedures. This section describes the agency's approach to a consistent and repeatable approach to managing incidents. It includes sections on:
  - Roles and responsibilities
  - Incident-related information collection
  - Updating policies with lessons learned
  - Collection of evidence
  - Incident response training
  - Document and artifact retention



## G.8 Secure Coding

### Secure Coding

This appendix documents a source of information on best practices and standards for secure coding. With the increased use of software products and the rapid pace of modern software development, it is essential to discover and resolve insecure software risks. The mitigations and guidelines to reduce these common risks can be found in secure coding best practices.

Understanding how software applications work can be a daunting thing; however, it could be key to know if data security is in jeopardy. Awareness of secure coding practices allows an agency to review potential vendors and their products prior to purchase and implementation. It also empowers the agency with the knowledge of the questions to ask a vendor of how the software was developed and whether the vendor uses secure coding practices or standards.

Additionally, the information in this appendix can provide a path forward for agencies with the internal capability to produce “in-house” software applications. By implementing security during the code writing process, security is “baked in” and there is more trust the software will aid in protecting the information it processes.

#### **Open Web Application Security Project (OWASP) Foundation**

The OWASP Foundation is a not-for-profit charitable organization focused on improving the security of software. OWASP operates as a community of like-minded professionals to provide unbiased and practical information about application security (AppSec) through software tools and documentation. These materials are available under a free and open software license, which can be located at the link below.

[https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)

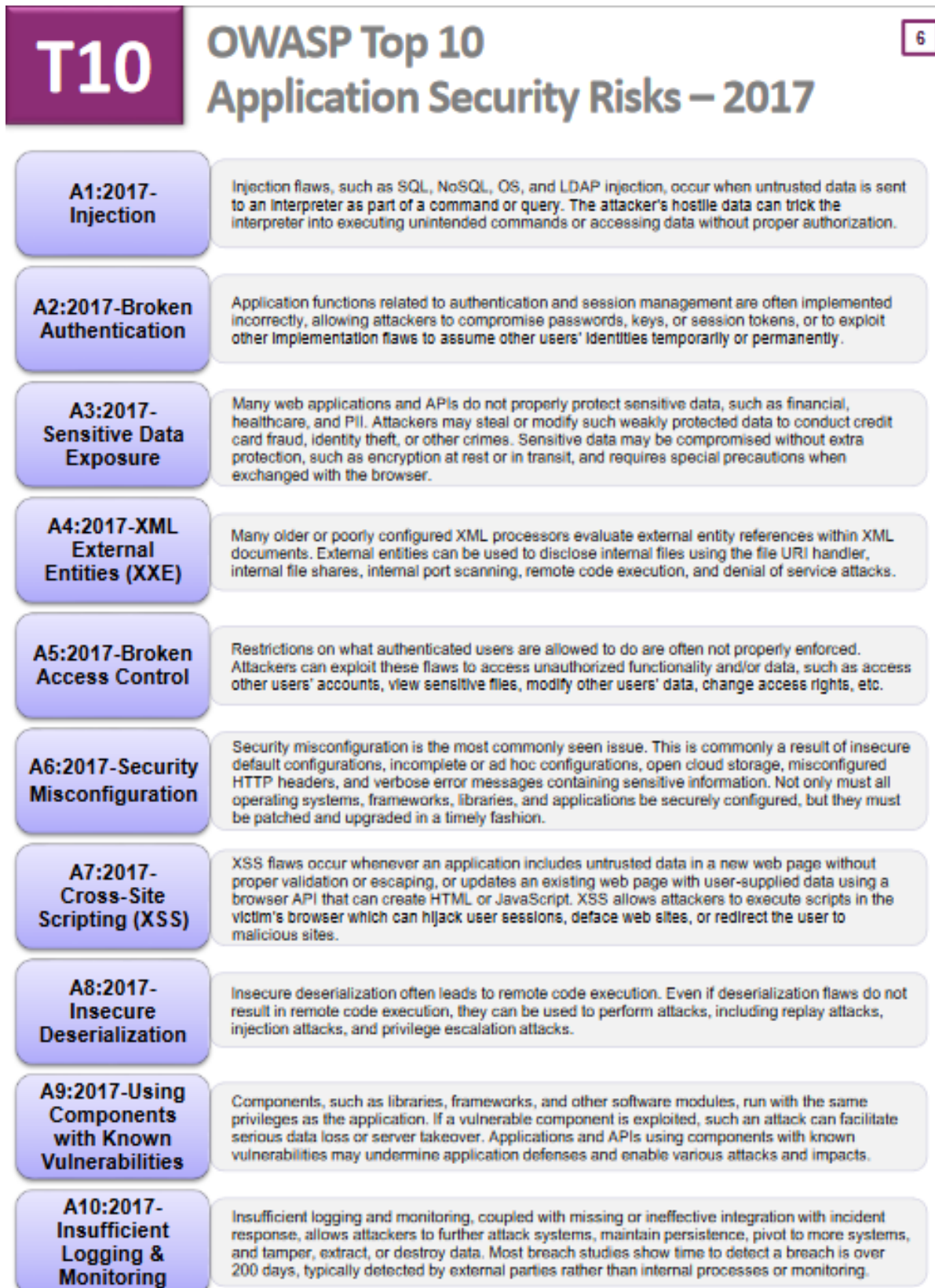
Software is becoming increasingly complex and connected, and the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.

The OWASP Foundation publishes the Top 10 Application Security Risks, which focus on the most serious web application security risks. The OWASP Top 10 is based primarily on 40 plus data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real world applications and application program interfaces (API). The Top 10 items are selected and prioritized according to this data, in combination with consensus estimates of exploitability, detectability, and impact.

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on a path forward.

The OWASP Top 10 focuses on identifying the most serious web application security risks for a broad array of organizations. For each of these risks, generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology.

Figure G.8-A



Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. It is critical to understand the risk to your organization based on applicable threat agents and business impacts.

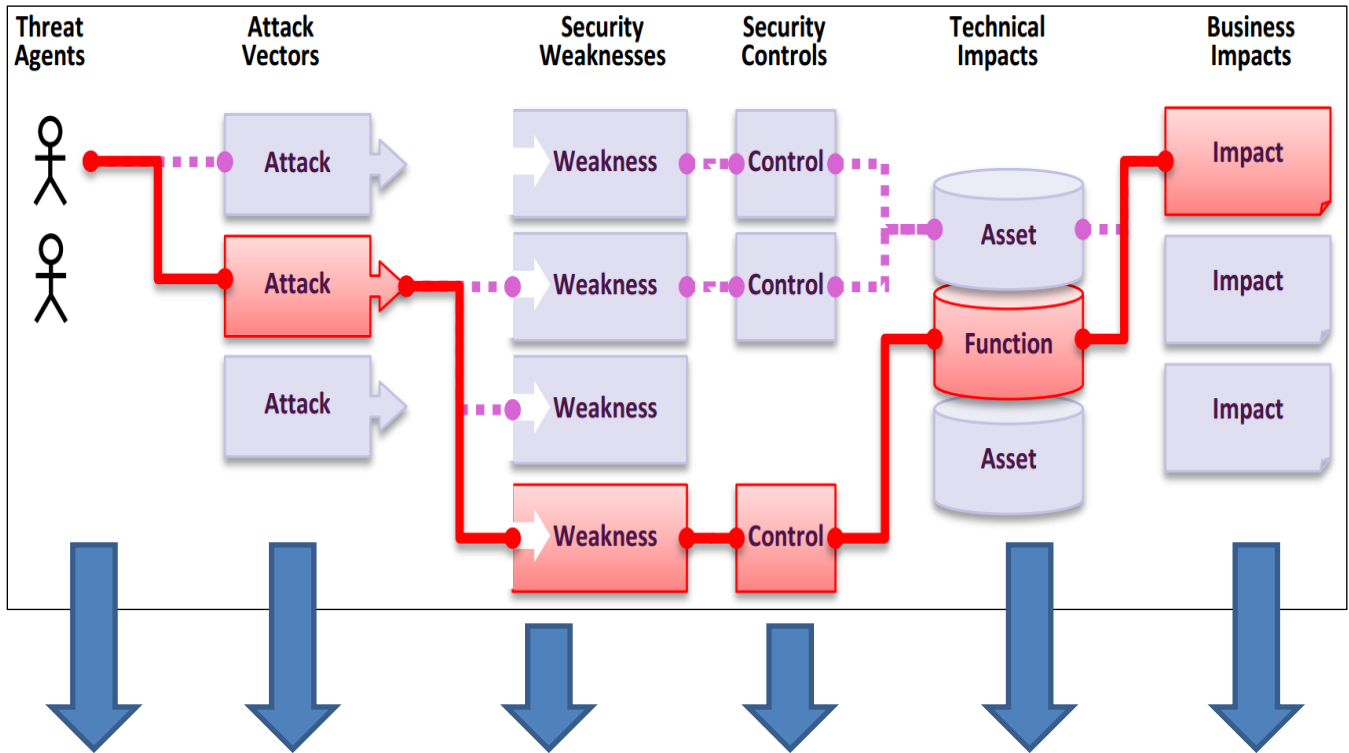
### **Application Security Risks**

The figures immediately below illustrate the path of a sample threat beginning with the threat agent and ending with the target or affected business resource. Various paths are available but the agent would normally select the path of least resistance which would be the most vulnerable and with the fewest number of effective security controls.

The sample risk matrix can be used to assign in the various aspects of potential vulnerability. Each column corresponds to a phase in the attack process. In the matrix, a lower value represents less risk and is more desirable.

Concerning secure coding practices, when security is built-in during code development, vulnerabilities can be identified and controls included reducing the overall risk to information processed by the code.

Figure G.8-B Sample Threat Path



Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	<b>EASY: 3</b>	<b>WIDESPREAD: 3</b>	<b>EASY: 3</b>	<b>SEVERE: 3</b>	App / Business Specific
	<b>AVERAGE: 2</b>	<b>COMMON: 2</b>	<b>AVERAGE: 2</b>	<b>MODERATE: 2</b>	
	<b>DIFFICULT: 1</b>	<b>UNCOMMON: 1</b>	<b>DIFFICULT: 1</b>	<b>MINOR: 1</b>	

Figure G.8-C General Risk Matrix

To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even severe software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved. The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors that have been assigned to each risk.

Figure G.8-D Top 10 Risk Factor Summary

RISK	Attack Vectors		Security Weakness		Impacts		Score
	Threat Agents	Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Whether you are new to web application security or already very familiar with these risks, the task of producing a secure web application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this task can be daunting.

To help organizations, developers, testers and managers reduce their application security risks in a cost-effective manner; OWASP has produced numerous free and open resources that you can use to address application security in your organization. The following are some of the many resources OWASP has produced to help organizations produce secure web applications and APIs.

### **Get Started:**

- Document all applications and associated data assets.
- Larger organizations should consider implementing a Configuration Management Database (CMDB).
- Establish an application security program to conduct analysis to define key improvement areas and an execution plan.

### **Risk Based Portfolio Approach:**

- Identify the protection needs of your application portfolio from a business perspective.
- Establish a common risk-rating model with a consistent set of likelihood and impact factors reflective of your organization's tolerance for risk.
- Measure and prioritize all applications and APIs and add results to CMDB.

### **Enable with a Strong Foundation:**

- Establish a set of policies and standards that provide an application security baseline for all development teams to adhere to.
- Define a common set of reusable security controls that complement these policies and standards and provide design and development guidance on their use.

### **Integrate Security into Existing Processes:**

- Define and integrate secure implementation and verification activities into existing development and operational processes.
  - Activities include threat modeling, secure design and design review, secure coding and code review, penetration testing, and remediation.

**Application Security Requirements** - to produce a secure web application, you must define what secure means for that application.

- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)  
<https://www.owasp.org/index.php/ASVS>
- [OWASP Secure Software Contract Annex:](https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)  
[https://www.owasp.org/index.php/OWASP\\_Secure\\_Software\\_Contract\\_Annex](https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)

**Application Security Architecture** - retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start.

- OWASP Prevention Cheat Sheets:

[https://www.owasp.org/index.php/OWASP\\_Cheat\\_Sheet\\_Series](https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series)

**Standard Security Controls** - building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs.

- OWASP Proactive Controls:  
[https://www.owasp.org/index.php/OWASP\\_Proactive\\_Controls](https://www.owasp.org/index.php/OWASP_Proactive_Controls)

**Secure Development Lifecycle** - to improve the process your organization follows when building applications and APIs, organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

- OWASP Software Assurance Maturity Model (SAMM):  
[https://www.owasp.org/index.php/OWASP\\_SAMM\\_Project](https://www.owasp.org/index.php/OWASP_SAMM_Project)
- OWASP Application Security Guide for CISOs:  
[https://www.owasp.org/index.php/Application\\_Security\\_Guide\\_For\\_CISOs](https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs)

**Application Security Education** – hands-on learning about vulnerabilities to help educate developers on web application security.

- OWASP Education Project:  
[https://www.owasp.org/index.php/Category:OWASP\\_Education\\_Project](https://www.owasp.org/index.php/Category:OWASP_Education_Project)
- OWASP WebGoat:  
<https://www.owasp.org/index.php/WebGoat>
- OWASP Broken Web Application Project:  
[https://www.owasp.org/index.php/OWASP\\_Broken\\_Web\\_Applications\\_Project](https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project)

**Understand the Threat Model** – be sure to understand the priorities when it comes to threat model.

- OWASP Testing Guide:  
[https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project)
- [Application Security Verification Standard \(ASVS\):](https://www.owasp.org/index.php/ASVS)  
<https://www.owasp.org/index.php/ASVS>

**Testing Strategies** – choose the simplest, fastest, most accurate technique to verify each requirement.

- OWASP Security Knowledge Framework:  
[https://www.owasp.org/index.php/OWASP\\_Security\\_Knowledge\\_Framework](https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework)



- [Application Security Verification Standard \(ASVS\):  
https://www.owasp.org/index.php/ASVS](https://www.owasp.org/index.php/ASVS)

## **APPENDIX H SECURITY ADDENDUM**

---

The following pages contain:

The legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4);

An example of a contract addendum (H-5);

The Security Addendum itself (H6-H7);

The Security Addendum Certification page (H8).

**FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES  
SECURITY ADDENDUM**

**Legal Authority for and Purpose and Genesis of the  
Security Addendum**

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.

We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.

The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

- a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
  - 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
  - 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
  - 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

**EXAMPLE OF A CONTRACT ADDENDUM**

AMENDMENT NO. \_\_\_\_ TO THE CONTRACT BETWEEN  
[PARTY NO. 1] AND [PARTY NO. 2], ENTERED INTO [DATE]

[Name of Law Enforcement Agency] and [Party No. 2], upon notification and pursuant to Paragraph/Section No. \_\_\_\_ [the amendment clause of the original contract] of that certain contract entered into by these parties on [date][and entitled "\_\_\_\_"], hereby amend and revise the contract to include the following:

1. Access to and use of criminal history record information and other sensitive information maintained in [state and] FBI-managed criminal justice information systems by [private party] are subject to the following restrictions:

- a.
- b.
- c.

and

d. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein.

This amendment is effective the \_\_\_\_ day of \_\_\_\_\_, 20\_\_.

On behalf of [Party No. 1]: \_\_\_\_\_

[Name]

\_\_\_\_\_

[Title]

\_\_\_\_\_

Date

On behalf of [Party No. 2]: \_\_\_\_\_

[Name]

\_\_\_\_\_

[Title]

**FEDERAL BUREAU OF INVESTIGATION**  
**CRIMINAL JUSTICE INFORMATION SERVICES**  
**SECURITY ADDENDUM**

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306



**FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES  
SECURITY ADDENDUM**

**CERTIFICATION**

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

\_\_\_\_\_  
Printed Name/Signature of Contractor Employee

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed Name/Signature of Contractor Representative

\_\_\_\_\_  
Date

\_\_\_\_\_  
Organization and Title of Contractor Representative

## APPENDIX I REFERENCES

---

- White House Memo entitled “Designation and Sharing of Controlled Unclassified Information (CUI)”, May 9, 2008
- [CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306
- [CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010
- [FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306
- [FISMA] *Federal Information Security Management Act of 2002*; House of Representatives Bill 2458, Title III–Information Security
- [FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004
- [FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006
- [FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1
- [NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14
- [NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25
- [NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36
- [NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32
- [NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34
- [NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35
- [NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36
- [NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39
- [NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

- [NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44
- [NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2
- [NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46
- [NIST SP 800–48] *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*; NIST Special Publication 800–48
- [NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52
- [NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2
- [NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A
- [NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58
- [NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT
- [NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT
- [NIST SP 800–64] NIST Special Publication 800–64
- [NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)*; NIST Special Publication 800–66
- [NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68
- [NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70
- [NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72
- [NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1
- [NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76
- [NIST SP 800–77] *Guide to IPsec VPNs*; NIST Special Publication 800–77
- [NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78
- [NIST SP 800–81] *Secure Domain Name System (DNS) Deployment Guide*; NIST Special Publication 800–81
- [NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

- [NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86
- [NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87
- [NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96
- [NIST SP 800–97] *Guide to IEEE 802.11i: Robust Security Networks*; NIST Special Publication 800–97
- [NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121
- [NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124
- [NIST SP 800-125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800-125
- [NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144
- [NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145
- [NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146
- [OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996
- [OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003
- [OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006
- [OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006
- [OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006
- [OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Meme 07–16; May 22, 2007
- [Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004
- [USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code,  
Title 44 - Public Printing and Documents; Chapter 35 - Coordination of  
Federal Information Policy; Subchapter I - Federal Information Policy, Section  
3506

## **APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE**

---

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Noncriminal Justice Agencies (NCJA) with access to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau (SIB) and/or Channeling agency. Examples of the target audience for the Appendix J supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those NCJAs new to the CSP and Advisory Policy Board (APB) auditing process (all NCJAs will be periodically audited by the CJIS Systems Agency (CSA)/SIB and may be included in a sampling of triennial audits conducted by the FBI) it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every NCJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

### **General CJI Guidance**

The following information provides NCJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. **3.2.9 – Local Agency Security Officer (LASO)**

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local NCJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and

procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.6 – Agency User Agreements

When an NCJA (private or public) is permitted to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions as authorized pursuant to federal law or state statute approved by the U.S. Attorney General, the information received from the background check, such as criminal history record information (CHRI) or personally identifiable information (PII), must be protected as CJI. In order to receive access to CJI the NCJA must enter into a signed written agreement, i.e., an agency user agreement, with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the CJI access. An example of a NCJA (private) is a local bank. An example of a NCJA (public) is a county school board.

*Note 1: The CSA, SIB, or authorized agency providing the CJI access term should be part of the agency user agreement.*

*Note 2: Any NCJA that directly accesses FBI CJIS must allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.*

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2.1.1 – All Personnel (Security Awareness Training)

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

*Note: The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.*

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help NCJAs with:

- (i) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (ii) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

*Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.*

*Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.*

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

*Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative*



*to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.*

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Electronic media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a criminal justice conveyance, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

*Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.*

*Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.*

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

*Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record*

*information for the purposes of licensing or employment need to follow the guidance in Section 5.12 (referenced below).*

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

*Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law.*

**The following scenarios are intended to help the reader identify areas within the CSP that NCJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above General CJI Guidance section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.**

**Hard Copy CJI Storage and Accessibility**

When an NCJA receives CJI via a paper copy from a CJA and stores the paper within a locked file cabinet, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

**Electronic CJI Storage and Accessibility – Controlled Area**

When an NCJA creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control – Encryption

CSP Section 5.5.2.4 item 3 – Encryption describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the

appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

### **Electronic CJI Storage and Accessibility – Physically Secure Location**

When an NCJA receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency’s environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

### **Use Case Scenarios**

#### **1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server**

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that has indirect access to CJI and is located in a secure data center within the board of education offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to an employee's electronic record. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the record, the user is prompted to enter their unique username and password. Because the record resides on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required to access the record.

*NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.*

## 2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) encryption algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access an employee's record, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder.

*NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.*

# APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

---

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance is not intended for criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as “terminal agencies”.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to criminal justice information (CJI) maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those CJAs new to the CSP it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every CJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific “shall” statement please go to the referenced section within the main body of the CSP.

## **General CJI Guidance**

The following information provides CJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. **3.2.9 – Local Agency Security Officer (LASO)**

It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

The LASO serves as the primary point of contact (POC) between the local CJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI must enter into a signed agreement with the CSA providing the access. The agreement specifies the services and systems the agency will access. It must also specify all pertinent governance policies to which the agency must adhere.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2 – Security Awareness Training

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

CSP Section 5.2.1.2 describes the topics required to be discussed for personnel that have both physical and logical access to CJI. These topics are covered in addition to the ones addressed in basic security awareness training.

CSP Section 5.2.1.3 describes topics to be covered for those personnel assigned information technology roles. Topics covered in this section are in addition to the topics addressed in Sections 5.2.1.1 and 5.2.1.2.

*Note: The CSO may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.*

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help CJAs with:

- (iii) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,
- (iv) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

*Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.*

*Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.*

f. 5.4 – Auditing and Accountability

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

*Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.*

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient.



The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to digital and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

“Digital media” is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. “Physical media” refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store digital and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn’t possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy digital media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a police vehicle, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data “at rest”) of CJI.

i. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 explains the technical safeguards ranging from boundary and transmission protection to security an agency’s virtualized environment.

CSP Section 5.10.1.2 details the requirements for the encryption of CJI whether in transit or at rest. FIPS 140-2 certification is required when CJI is in transit outside a physically secure location. When at rest outside a physically secure location, encryption methods can use Advanced Encryption Standard (AES) at 256 bit strength or a FIPS 140-2 certified method.

CSP Section 5.10.3 explains the use of virtualization and partitioning when processing CJI in a virtual environment. A virtualized environment can be configured such that those parts of the system which process CJI are either physically or virtually separated from those that do not.

CSP Section 5.10.4 explains system and information integrity policy and procedures. This includes areas such as patch management, malicious code protection, and spam and spyware protection.

j. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

*Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.*

*Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.*

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one

representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

k. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

l. 5.13 – Mobile Devices

When access to CJI using mobile devices such as laptops, smartphones, and tablets is authorized, CSP Section 5.13 explains the controls required to manage those devices to ensure the information remains protected.

**The following scenarios are intended to help the reader identify areas within the CSP that CJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above “General CJI Guidance” section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.**

**Hard Copy CJI Storage and Accessibility**

When CJI is received in hard copy and the agency stores the paper within a locked file cabinet, the CJA should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

**Electronic CJI Storage and Accessibility – Controlled Area**

When an agency creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control Mechanisms – Encryption

CSP Section 5.5.2.4 item 3, Encryption – This describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this

situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

### **Electronic CJI Storage and Accessibility – Physically Secure Location**

When an agency receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the agency should, in addition to the “General CJI Guidance”, focus on compliance with policy sections:

a. **5.5 – Access Control**

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. **5.6 – Identification and Authentication**

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. **5.7 – Configuration Management**

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. **5.10 – System and Communications Protection and Information Integrity**

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency’s environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

## Use Case Scenarios

### 1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county court scans hard copy case documents containing CJI into an electronic format. The documents are placed on a network server which is located in a secure data center within the court offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to case documents. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the documents, the user is prompted to enter their unique username and password. Because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

*NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.*

### 2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

A county court scans hard copy case documents containing CJI in an electronic format. The documents are placed on a network server which is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access to the case documents, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder. Additionally, because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

*NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.*

***TEAGUE***

***POLICE DEPARTMENT***



**Field Training  
Program Manual**

# TABLE OF CONTENTS

<b>CHAPTER 1</b>		
	<b>INTRODUCTION AND PROGRAM OVERVIEW</b>	<b>3</b>
<b>CHAPTER 2</b>		
	<b>FTO SELECTION PROCESS</b>	<b>9</b>
<b>CHAPTER 3</b>		
	<b>MANAGEMENT OF THE FIELD TRAINING PROGRAM</b>	<b>12</b>
<b>CHAPTER 4</b>		
	<b>PROGRAM OPERATING PROCEDURES</b>	<b>17</b>
<b>CHAPTER 5</b>		
	<b>STANDARD EVALUATION GUIDELINES</b>	<b>42</b>
<b>CHAPTER 6</b>		
	<b>REMEDIAL TRAINING</b>	<b>54</b>
<b>CHAPTER 7</b>		
	<b>TERMINATION PROCEDURES</b>	<b>69</b>

# **CHAPTER 1**

## **INTRODUCTION AND PROGRAM OVERVIEW**



## **FIELD TRAINING PROGRAM**

### *INTRODUCTION*

The Teague Police Department Field Training Program is an approach to the field training of recruit officers based on a system of formal, standardized and structured teaching and evaluation. The demands placed on police officers today require them to gain a vast amount of knowledge. To be effective and safe, they must learn and be able to relate that knowledge to field situations. The learning process, which begins in the classroom at the Police Academy, will continue to be integrated with practical field instruction. The result will be a recruit who has been thoroughly trained and who is confident and efficient.

The Field Training Program is a vital part of the total selection process of a police officer. Only when the pre-employment selection process, the academy training, and the field training are based on fair and equitable standards is the system valid. The demand for a standardized field-training program is clear and necessary if it is to be a part of the selection process. The courts, community groups, and the recruits themselves have and will challenge an inadequate or faulty system. The Field Training Program is designed to meet these challenges.

The Program requires four groups of people to combine their efforts to ensure its success. The Recruits, the Field Training Officers, and the FTO Supervisor.

The recruit, being the primary target of the Program, undergoes sixteen (16) weeks of field training, broken down into four phases. The objective of the Program is to produce a police officer at the end of this sixteen-week period, which can function in a safe, skillful, and professional manner. Documentation checklists guide the instruction.

The first phase is four (4) weeks long, beginning with two (2) days of orientation, during which the recruit is not evaluated. The second and third phases are five (5) weeks in duration. Should there be correctable problems, the recruit may be reassigned to an FTO for remedial training. The recruit then enters a two-week evaluation-only phase, the fourth and final phase and is commonly referred to as the "Ghost Phase." After passing his

evaluation, he is assigned to patrol to complete probation. Only when it has been demonstrated that the standards can be met is a recruit graduated from field training to full duty. Should the recruit be unable to meet the standards, termination may result. The documentation to support the FTO, Supervisor, and Department should be present and capable to stand the test of validity.

The Field Training Officer is the coach, instructor, documenter, evaluator, and the key to the Program. The training of the recruit places greater demands on the FTO. Therefore, the selection process of the FTO is demanding. The process requires an application, an appraisal recommendation by supervisors through the chain of command and found acceptable by the Chief of Police.

The FTO Supervisor is a coach, documenter, motivator, and evaluator. His interest and dedication are of paramount importance for the success of the Program. The FTO Supervisor must be a Team Player that is supportive of the Command Staff and their ideologies toward improving training and creating a professional department. This individual must be capable of seeing the big picture and to put aside all personal feelings regarding recruits FTO's or any other member of this department. The FTO Supervisor must be able to multi-task and at the same time keep an open mind in a constant changing environment. It is essential that the FTO Supervisor follow the chain of command at the same time be willing to identify a potential problem, providing possible solutions and bring those issues and solutions to the Chief of Police. Working closely with staff as well as the recruit and FTO, he observes, corrects, and guides both toward their goals. As an evaluator, he can measure both the recruit and FTO. He reviews, compiles, and monitors all recruit evaluations ensuring fairness and impartiality. Through frequent contact, he will be the synthesizing factor to relate the Program objectives to the recruit and FTO. The FTO Supervisor should also derive satisfaction from the knowledge that his efforts today dramatically affect the quality of our Department in the future.

The combined efforts of all personnel who are a part of the Program are necessary to ensure its success. While only a few are directly involved, indirectly every member of the Department will benefit to some degree. The success of the Field Training Program will be evident for years to come through the professional police officers developed by the Teague Police Department.

## ***INDOCTRINATION TO TRAINING***

The Recruit's first few days in the Field Training Program are the most critical from the standpoint of learning and development. It is during this period that important attitude and behavior patterns are established. During the first days of training, the Recruit forms permanent attitudes. This is also the time when the Recruit learns what is expected during training, and during his whole patrol career. The Recruits expect to be challenged, and they expect to be properly trained by superiors. Any comments superiors make about them or about their performance will likely be taken very seriously. They will be very concerned about meeting the requirements of the Training Program and following the instructions of the FTO. They all want to succeed.

Even though a Recruit should be expected to conform to the training regimen, the FTO should realize that there are natural forces that work on the Recruit that make his first days in training more difficult than they would otherwise be as well as decrease the quality of their performance. The recruit is faced with starting a new job, or for the recruit, who comes from another shift, he is faced with starting a new situation. To compound the situation, many new recruits are starting their first real jobs. They do not have prior work experience to guide their behavior and performance. They do not know what to expect either.

The FTO's should remember how they felt when they began training and will better appreciate the Recruit's predicament. The Recruit's problems and fears can be allayed by the simple application of a little understanding by the FTO. The Recruit should not be pampered, but should be treated in a realistic, understanding manner.

During the initial orientation process, the FTO should also establish a friendly, open, and professional rapport with the Recruit. Development and learning come through effective communication. Rapport is important to communication because people are not likely to share their ideas, questions, or feelings unless they feel their listener is open or sympathetic to their conversation.

The FTO should also convey a positive attitude that the Recruit can succeed in the Program. A Recruit needs to know that the FTO wants him to succeed

and that the FTO will help him to succeed. Everyone needs to know that they have an even chance of success.

It is particularly important that an FTO maintain a positive and objective attitude when a Recruit is received who has not performed well with another FTO. The new FTO should give the Recruit every opportunity to succeed. The FTO should not be prejudiced based on prior performance or rumors. He should base all judgments on independent observations, not on another's comments. It is entirely possible that the change of FTO's and the application of a positive attitude by the new FTO may in themselves be sufficient to elicit acceptable performance from the Recruit. The emphasis should be put on developing a viable, competent police officer.

Sufficient flexibility has been designed into the Program so that individual needs of the Recruit and that overall needs of the Department can both be met. It is incumbent upon the supervisor and the FTO to work within acceptable limits and to apply an individual training approach to each recruit so that he can fully develop during training. Again, the atmosphere should be one in which the Recruit has the maximum opportunity to succeed.

The FTO should use training methods that are conducive to producing a successful Recruit. This latter point cannot be overemphasized. All too often, ineffective or counterproductive stress-training methods are used. The use of loud profanity, table pounding, or humiliation tactics should not be relied upon. These methods do not contribute to good learning, nor do they place the Recruit in a proper state of mind. They have no place in the daily training routine. Instead, an FTO should seek to reinforce the positive attributes or accomplishments, rather than to constantly downgrade the weaknesses.

Remember that people respond much more quickly to a positive statement than to a negative one. Above all, within the limits of good judgment, an FTO should use good, realistic, and established training methods that are conducive to the Recruit's needs and development as a patrol officer.

In summary, the FTO should recognize that the first few days of training are critical. The FTO must apply an effective orientation process that adequately considers the very real and natural forces that serve to lessen a Recruit's

performance. The FTO Team should work to create a positive learning environment that suits the individual characteristics and development of the Recruit. Above all, the FTO Team should use a selection of good, reliable, and acceptable training techniques that are most conducive to producing a viable, competent police officer with a professional orientation.

# **CHAPTER 2**

## **SELECTION PROCESS**

## FIELD TRAINING OFFICER

### INTRODUCTION

The Field Training Officer must have the combined skills of an experienced police officer and a patient teacher/coach. He must be a leader and a “Role Model” not only for the Recruit but his peers as well. The FTO’s job is particularly difficult because he will be required to supervise the Recruit but temper this supervisory image with empathy for the new employee. Motivation and innovation are two other character traits that the FTO should possess and pass on to the Recruit. With these responsibilities in mind, one can see why the selection process is vital and must cover numerous aspects of the officer’s past and present career as well as his attitudes and expectations for the future.

The following pages of this chapter outline and explain the selection process of the Field Training Program. Adherence to this process coupled with dedication and determination by those involved in it will ensure the appointment of only the most qualified personnel to the position of Field Training Officer.

### MINIMUM REQUIREMENTS

The following requirements must be met before the FTO is permitted to train a recruit:

- A. Two years of service with the Teague Police Department as a commissioned officer.
  - 1. Officers with less than two years can be considered if the needs of the Department warrant the selection.
- B. Must be recommended by their chain of command.
- C. New applicants meeting the requirements will be interviewed by the Chief. If an applicant was an FTO before, they will be considered by the Chief.
- D. Applicants selected to become FTOs must successfully complete:
  - 1. An approved FTO school or be approved by the Chief of Police.

## **FTO SELECTION PROCESS**

- A. Selection of Field Training Officers will be based on the best officers available for the assignment and those that represent the true mission and values of the department.
- B. When an opening exists, the Chief of Police will solicit recommendations from departmental supervisors.
- C. The Chief will review prior performance evaluations, activity levels, any complaints and commendations as well as advanced training.
- D. The Chief will interview potential candidates and decide based on the best interests of the department.

## **REMOVAL / WITHDRAWAL FROM PROGRAM**

- A. Officers who fail to perform satisfactorily in the FTO position will be removed from the program by the Chief of Police.
- B. Officers who want to withdraw from the FTO program should submit a memo to the Chief indicating their desire to withdraw. The memo should be routed through the Sergeant on the officer's shift and to the FTO Supervisor. That memo will then be forwarded to the Chief of Police.



**CHAPTER 3**

**MANAGEMENT OF**

**THE FIELD TRAINING PROGRAM**

## **FIELD TRAINING PROGRAM**

### ***INTRODUCTION***

Management of the Field Training Program requires the cooperative effort of all members of the Patrol Division.

The recruit will be assigned to the Patrol Division to continue training which began at the Police Academy. The FTP, being the next step in training, is designed to provide each recruit the necessary instruction and guidance to meet the standards of the Department. The Academy prepares the recruits through classroom instructions and simulation exercises. The FTP will complement and build on this preparation through field instructions. The recruit and all supervisors should view the sixteen (16) weeks of field training as part of the total selection process of becoming a Teague Police Officer.

The management of the Field Training Program as discussed in this chapter is intended to guide and aid in coordination of the Program. One objective of the Program is to standardize the field training of all recruits and develop consistency throughout the program. Only by employing guidelines set out in this chapter can the objectives be achieved.

***RECRUIT ORIENTATION (By the FTO Supervisor on first day of Field Training)***

- A. The orientation should include, but is not limited to, the following:
  - 1. The philosophies of the Department should be conveyed.
  - 2. The FTO's role and responsibilities in relation to the recruit and the program
  - 3. Steps the recruit may take to resolve conflicts or receive assistance to problems encountered during training.
  - 4. He should be informed again of the reporting time to his assigned duties, and what rotation schedule he will follow.
  - 5. The shift supervisor should add to this orientation, items that are of importance to his shift.
  
- B. During the orientation, the orientation form contained in the Recruit Officers Training Manual will be completed and signed. The form will remain in the manual and be a part of the Training File. (See Form 3-1)

## ORIENTATION

1. The Field Training Officer is your immediate "supervisor". You will always follow his directions/orders during any police incident. He is responsible. If you have any questions regarding the actions he has you take, discuss them with the Field Training Officer when the incident has been concluded.
2. If at any time you and the Field Training Officer do not agree and cannot resolve the dispute, both will report to the FTO Supervisor.
3. Maintenance of the Field Training Guide is your responsibility.
4. It is always your responsibility to know if you are or are not making satisfactory progress in your training. The Field Training Officer will be keeping documentation daily of your progress, strengths and/or weaknesses.
5. You will adhere to the City and Departmental Policy Manual, along with the Standard Operating Procedures, by immediately reporting to a supervisor, infractions occurring in your presence.

6. Reporting Date \_\_\_\_\_ Time \_\_\_\_\_

SIGNED: Recruit Officer \_\_\_\_\_

Date \_\_\_\_\_

I have explained the above items to Recruit Officer \_\_\_\_\_

SIGNED: FTO Team Supervisor \_\_\_\_\_

Date: \_\_\_\_\_

(FORM 3-1)

## ***RECRUIT PHASE ROTATION***

- A. The recruits will be assigned to an FTO by the FTO Supervisor.
- B. Each recruit will rotate through the following schedule:
  - 1. Phase I Four (4) weeks FTO 1
  - 2. Phase II Four (4) weeks FTO 2
  - 3. Phase III Four (4) weeks FTO 3
  - Phase IV Four (4) weeks FTO 1 (Ghost Phase)
- D. A remedial training assignment approved by the FTO Supervisor may be made with any FTO.
- E. Should a recruit require intensive remedial training, he may be removed at any point in Phase I through II for a period not to exceed four weeks. The Daily Observation Report will reflect which phase the recruit is in. (Example - "Phase 2 IRT - Wk 1")

# **CHAPTER 4**

## **PROGRAM OPERATING PROCEDURES**

# **FIELD TRAINING PROGRAM**

## ***PROGRAM STRUCTURE AND DURATION***

The recruit will be introduced to the Field Training Program, after being hired by the Board of Alderman. Actual field training with an FTO will begin as soon as possible. The Program will then continue for approximately sixteen (16) weeks.

The Field Training Program is divided into four periods, which will be known as "phases." Each phase, except Phase IV, may find the recruit with a different FTO. At the inception of Phase IV, the recruit transfers back to their original FTO for an "Evaluation Only" phase, unless a transfer or serious problem prevents their return.

In the following paragraphs, the four phases are identified and explained:

### Phase I

The first two days of Phase I is known as an "Orientation Period." During this interval, the recruit will not be evaluated by the FTO or the sergeant.

At any time during field training, the FTO may clear "one-man, with a recruit observer," to ensure that adequate coverage is assigned to calls for service. This option is important to the FTO until they can adequately assess the capabilities of their assigned recruit. The recruit trains in Phase I with the first FTO for four calendar weeks.

### Phase II

During the final weeks of Phase I, the recruit will be informed of their training assignment for Phase II. It will be the responsibility of the FTO Supervisor to determine the recruit's days off and the date to report for duty.

The FTO and sergeant should ensure that the recruit has had adequate exposure and is progressing satisfactorily before they can complete Phase II. The recruit must receive a rating of four (4) or better in all rating categories on the Phase II End-of-Phase Evaluation report to proceed into Phase III

During Phase II, it is a logical place to remove the recruit from the Program schedule and inject them into remedial training if they are demonstrating a

deficiency that must be overcome before Program completion. In fact, this must be done if the recruit would not receive the required evaluation of all fours in all categories on the Phase II End-of-Phase Evaluation Report. Phase II is four calendar weeks in duration

### Phase III

Phase III is the last phase during which the recruit will receive intensive training from the FTO. Phase III is four weeks long. The recruit should be given more responsibility for handing calls start to finish during this period.

### Phase IV

The final period in the program is Phase IV, the "Evaluation only" phase. During Phase IV, the recruit is assigned to the Phase I FTO, if possible. Phase IV begins in the thirteenth week in the FTO Program and is two calendar weeks in length.

In Phase IV, the recruit will be expected to perform almost entirely on their own. The FTO will be along merely as an observer and evaluator but shall at all times maintain override discretionary control: i.e., they should intervene when necessary to preserve safety, the integrity of the Department, or prevent irreversible error on the part of the recruit. Otherwise, the FTO should allow the recruit considerable leeway and encourage initiative and independent action by the recruit. To adequately assess the recruit, the FTO may clear "one-man with an FTO Observer" to allow the recruit to function in a "one-man" status.

## *ABBREVIATED PROGRAM AND REQUIREMENTS FOR ACCEPTENCE*

To be eligible for participation in the Teague Police Department's abbreviated program, the Recruit will have been a certified Peace Officer immediately prior to being hired and working as a Peace Officer in a job with duties similar to those of a Teague Police Officer for at least two years. The Recruit will start the Abbreviated Training Program, which will be two weeks in Phase 1, two weeks in Phase 2, two weeks in Phase 3, and two weeks in Phase 4, for a total of eight weeks.

If at the end of Phase 1 the Recruit is not scoring "4" or better on all



categories of the DOR, the Recruit will be removed from the Abbreviated Training Program and commence the normal 16-week training cycle. During the Abbreviated Training Program, the Recruit can be allowed two weeks of IRT. If that time is insufficient the Recruit will commence with the 16-week training program at the appropriate point in the training cycle.

## ***RECRUIT SCHEDULING***

This program is built on a foundation of consistency and standardization. The program cannot set a specific policy on how many FTO's a recruit should work with. There are too many variable factors involved to establish a strict guideline. The FTO Supervisor has the primary responsibility for scheduling of the recruit to an FTO and should plan, using good judgment as their primary objective.

The FTO Supervisor must keep in mind that there is no problem in the FTO's taking leave time that is due them. However, the supervisor granting the leave should ensure that the recruit is not "bounced" from one relief FTO to another. Generally, supervisors granting leave of two or more days should schedule the recruit with a single relief FTO, if possible. If need be, the recruit's days off can be adjusted to meet this goal.

Recruit leave time should be kept to an absolute minimum. It is important that the recruit receive as much practical field exposure as possible during this training cycle. The recruit should be granted leave time (compensatory days) only when it is in the best interest of the recruit and the Department.

## ***THE CONCEPT OF TRAINING***

Before the Field Training Officer can begin to evaluate the recruit's performance, the FTO must establish their goals for the training of the recruit. Training is stressful, not only for the student, but for the teacher as well. Without a solid foundation to build upon, the transfer of experience and knowledge can become a taxing responsibility. The FTO's goals should boil down to two basic points:

- a. Teach the recruit how to apply the theory he has learned in the academic setting to the real world; and
- b. Teach the recruit how to be a good researcher, (i.e., where or who do they go to obtain information).

First, the FTO should realize that the hardest thing for a recruit officer to learn, might well be the ability to decide and then act on it. Laws, rules, and policies are necessary to function in a civilized world, but they cannot account for every possible situation where people are involved. The FTO must be able to pass their experience and judgment ability on the recruit.

Second, most individuals have a limited capacity to memorize and retain data. Memorization of information should be limited to areas of safety and repetitious work tasks. The department provides all officers with copies of our Policies, Texas Penal Code, SOP, etc. The recruit should have a working knowledge of all patrol policies and procedures. The recruit should be taught areas of expertise each unit has within the department. In other words, teach the recruit how to find information as well as developing memorization skills.

On-the-job training is difficult because it takes so much more patience to allow the student to perform the task. Not only does it take longer to accomplish the task, but at times can threaten the nerves or even safety of the trainer. Therefore, it is clear the FTO must have the dedication, commitment, and pride to mold the finest officers possible for the department.

## ***THE EVALUATION PROCESS***

## INTRODUCTION

Each recruit's progress as they proceed through the Program, is recorded through written evaluations. The evaluation process is equally as important as the training process, and, as such, has been given great attention.

Evaluations have many purposes, the obvious one being to record a recruit's progress; but there are others as well. Evaluations are excellent tools for informing the recruit of their performance level at a given point in time. They are also efficient devices for identifying training needs and documenting training efforts. In a word, evaluation represents feedback.

Collectively, over the duration of the Program, evaluations tell a story, both categorically and chronologically. They tell of a recruit's success and failures, improvements and digressions, and of the attempts to manage each of these occurrences. They chronicle skill and efforts of the FTO as well. Evaluations are critical in the career of each new officer and should be treated as such. **Honest and objective evaluations of recruits shall be a prime consideration of all members of this program.**

Under this program, only the performance of the recruit, that the FTO can note through their five (5) senses can be rated and thus documented. Performance noted outside the FTO's personal knowledge zone must be documented by those individuals involved. This documentation may be in a memorandum format or on a "Narrative Comments" continuation form, where another FTO observes the performance.

Each recruit will be evaluated over several categories. These categories cover as much as each aspect of the police environment and responsibilities as can be expected. The Teague Police Department has selected twenty-five categories as the basis for evaluating a recruit's performance while they are in the Program. These criteria which have formed the basis for recruit evaluation in police departments throughout the nation are found on the Teague police Department's "Observation Report." (See Form 4-1 and 4-2)

To ensure that the "Observation Report" and each rating of a recruit will be equally standard throughout the Department, Standardized Evaluation Guidelines have been established (See Chapter 5). The Standardized Evaluation Guidelines are behavioral anchors.

They provide a definition of unacceptable, acceptable, and superior levels of performance for each of the twenty-five categories. The standards set out in the "Guidelines" must be applied to all recruits regardless of their experience level or other incidental factors. By the strict application of the behavioral definitions contained in the "Guidelines", the rating of any given recruit performance by one FTO should match that of any other FTO. With this approach to evaluation, one may be assured that ratings through the Division are impartial, objective, uniform, and therefore, valid.

#### A. Evaluation Frequency

Sergeants' complete weekly evaluations while the recruit is in training with an FTO, the ultimate responsibility for evaluating a recruit's performance lies with the FTO.

Field Training Officers complete a daily evaluation on each recruit. The form used for this purpose is the "Observation Report." The "Observation Report" is a dual-purpose form in that it can be used for daily evaluations and end-of-phase evaluations by the FTO. This form must be completed at the end of each shift and not left, except for extraordinary circumstances, to a later time. This provides an opportunity for the recruit to ask questions that they failed to ask earlier in the day and serves to reinforce instructions and critiques that were given during or after each incident.

Daily Observation Reports (DOR's) are completed each day that the recruit works in the Field Training Program beginning with day one in Phase I and continuing through the last day of Phase IV. (See forms 4-1 and 4-2). Even though the recruit's first two days are orientation days, the DOR's will be completed in heading only and signed by the recruit and FTO. A notation, "Orientation Day" should be made of the form. Additionally, the FTO is responsible for submitting a D.O.R. for any absences other than regularly scheduled days off. The purpose of this is to document continuity and progression of the recruit through the schedule. A "Narrative Comments" continuation form is also available that can be utilized with any program forms (See Forms 4-3 and 4-4).

The second type of evaluation done by the FTO is the "End-of-Phase" (E.O.P.) evaluation. Submitted on the "Daily Observation Report" (D.O.R.) form, the "End-of-Phase" is a summation of the recruit's performance during the phase.

While produced on the same form, there is a distinct difference and purpose in the D.O.R. and E.O.P. reports. The D.O.R. is intended to be an objective appraisal of the recruit's performance for a specific day's work. The appraisal must be based on specific factual performance experienced by the FTO and recruit.

The E.O.P. is intended to be more of a cumulative appraisal, covering the overall performance of the recruit during that phase. This appraisal will assess the overall performance, capabilities, and remediation to date. Generally, the FTO should address the strengths and weaknesses in narrative form.

The FTO Supervisor is responsible for completing a weekly evaluation for the recruit while the recruit is in training with an FTO. This weekly evaluation is submitted on the "Weekly Observation Report" and is a collection of the sergeant's personal, first-hand observations of the recruit's performance (See Form 4-5). These first-hand observations may involve personal interaction with the FTO and recruit in resolving a deficiency. The Supervisor is not required to actually "observe a deficient performance" before addressing the item in their report. The main purpose of this report is that the first-line supervisor acknowledges the recruit's assignment, notes any personal interaction with the FTO and/or recruit, and makes a weekly overall assessment of the recruit's performance. The "Weekly Observation Report" will be submitted at the end of each training week. A training week is a full workweek, regardless of the days off the recruit, the FTO, or the Supervisor.

### PROBATIONARY OFFICER EVALUATION (After FTO Program)

Following the release of the recruit from the FTO Program, the assigned Patrol Sergeant will complete monthly observation reports and an end of probation report (using the monthly form) on the probationary officer (See Form 4-6, 4-7). This form of evaluation will be based on, but not limited to, the Sergeant's personal, first-hand observations of the recruit's performance. The first-hand observations may involve personal interaction with the recruit in resolving a deficiency. The Sergeant is not required to actually "observe a deficient performance" before addressing the item in their report. The Sergeant will use the appropriate categories of the Standard

Evaluation Guidelines to complete the report. The first monthly Observation Report will be submitted one month from the date the recruit was released from the Phase IV FTO. The monthly report will be submitted monthly until two weeks prior to recruit completing the probationary period. These reports will be kept in the probationary officer's training file.

## B. Flow of Evaluation Forms

After reviewing the Daily Observation Report with the FTO, the recruit will transpose the grades into the column on the far-left side of the front page. Any categories noted "Not Observed" will also be noted in this column. The recruit will then sign the appropriate block on the back of the Daily Observation Report and any continuation pages. In signing the Daily Observation Report (or End-of-Phase Report), the recruit is signifying that they have read and reviewed the report only. The recruit may not refuse to sign the report based on a disagreement in perception of performance with their FTO. Any disagreement with the FTO as it relates to factual circumstances that cannot be resolved will be brought to the FTO Supervisor.

The FTO will check the form for completeness and then forward the DOR to the FTO Supervisor. The original forms will all be maintained in the recruit's training folder.

The FTO Supervisor will present his completed Weekly Observation Report and Teague Police Observation Report (DOR) to the recruit with any explanation and/or counseling.

As with the D.O.R., the recruit will review the form and sign. The FTO Sergeant will forward the Weekly Observation Report with the DOR's to the Chief of Police.

The FTO's "End-of-Phase" reports, after being completed and signed, will receive a review through the chain of command up to the Chief, and then be filed in the recruit's training file.

### PROBATIONARY OFFICER (After FTO Program)

The assigned Patrol Sergeant will present the completed Monthly Observation Report and the End of Probation Report to the probationary officer with any explanation and/or counseling. The

reports will receive a review through the chain of command up to the Division Commander and will then be filed in the probationary officer's personnel file.

### SIX (6) MONTH PROBATIONARY PERIOD

A person appointed to a beginning position in the police department must serve a probationary period of six (6) months beginning on that person's date of employment as a police officer



RECRUIT \_\_\_\_\_ FTO \_\_\_\_\_ DIVISION/WATCH \_\_\_\_\_ DATE \_\_\_\_\_

RATING INSTRUCTIONS: Rate observed behavior on the scale below using the numerical value definitions contained in the standardized evaluation guidelines. You must comment on the most and least acceptable performance of the day. Although specific comments are required for all ratings of "1" or "6" and above, and "NRT", you are encouraged to comment on any behavior you wish. Use category numbers to reference your narrative comments. Check the "NO" box if a category is not observed. Check "NRT" box if the recruit fails to respond to training.

Assignment or Reason for No Evaluation:

	1	2	3	4	5	6	7	NO	NRT
<b>PERFORMANCE TASKS</b>									
_____ 1. Driving Skills: Normal Conditions.....	1	2	3	4	5	6	7	_____	_____
_____ 2. Driving Skills: Stress Conditions.....	1	2	3	4	5	6	7	_____	_____
_____ 3. Orientation/Response Time to Calls.....	1	2	3	4	5	6	7	_____	_____
_____ 4. Field Performance: Stress Conditions.....	1	2	3	4	5	6	7	_____	_____
_____ 5. Self-Initiated Field Activity/Observation Skills.....	1	2	3	4	5	6	7	_____	_____
_____ 6. Officer Safety.....	1	2	3	4	5	6	7	_____	_____
_____ 7. Control of Conflict: Verbal Skills.....	1	2	3	4	5	6	7	_____	_____
_____ 8. Control of Conflict: Physical Skills.....	1	2	3	4	5	6	7	_____	_____
_____ 9. Radio: Comprehension/Usage.....	1	2	3	4	5	6	7	_____	_____
_____ 10. Routine Forms: Accuracy/Completeness.....	1	2	3	4	5	6	7	_____	_____
_____ 11. Report Writing: Organization and Detail.....	1	2	3	4	5	6	7	_____	_____
_____ 12. Report Writing: Appropriate Time Used.....	1	2	3	4	5	6	7	_____	_____
_____ 13. Field Performance: Non-Stress.....	1	2	3	4	5	6	7	_____	_____
_____ 14. Investigative Skills.....	1	2	3	4	5	6	7	_____	_____
_____ 15. Interview/Interrogation Skills.....	1	2	3	4	5	6	7	_____	_____
_____ 16. Problem/Solving/Decision Making.....	1	2	3	4	5	6	7	_____	_____
<b>KNOWLEDGE</b>									
_____ 17. Departmental Policy/Procedures.....	1	2	3	4	5	6	7	_____	_____
_____ 18. Penal Code, Criminal Procedures, City Ord.	1	2	3	4	5	6	7	_____	_____
_____ 19. Vehicle Code.....	1	2	3	4	5	6	7	_____	_____
<b>ATTITUDE</b>									
_____ 20. Acceptance of Feedback/Following Instructions...	1	2	3	4	5	6	7	_____	_____
_____ 21. Attitude Toward Police Work.....	1	2	3	4	5	6	7	_____	_____
_____ 22. Relationship with Public in General.....	1	2	3	4	5	6	7	_____	_____
_____ 23. Relationship with Ethnic Groups.....	1	2	3	4	5	6	7	_____	_____
_____ 24. Relationship with Other Officers and Supervisors.	1	2	3	4	5	6	7	_____	_____
<b>APPEARANCE</b>									
_____ 25. General Appearance.....	1	2	3	4	5	6	7	_____	_____

MINUTES OF REMEDIAL TRAINING TIME \_\_\_\_\_

(Form 4-1)

(Explain under Additional Comments)

**NARRATIVE COMMENTS**

Most Acceptable  
Performance \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Improvement  
Needed \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Additional  
Comments \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

RECRUIT \_\_\_\_\_  
RATER \_\_\_\_\_  
.....

EVALUATION REVIEWS

SERGEANT \_\_\_\_\_

WATCHCOMMANDER \_\_\_\_\_

(FORM 4-2)

**TEAGUE POLICE DEPARTMENT**

**FIELD TRAINING PROGRAM**





DATE: \_\_\_\_\_ PHASE: \_\_\_\_\_ WEEK: \_\_\_\_\_

RECRUIT: \_\_\_\_\_ FTO: \_\_\_\_\_ WATCH: \_\_\_\_\_

GRADING SERGEANT: \_\_\_\_\_

HOW OBSERVATION WAS MADE: \_\_\_\_\_

COMMENTS:

\_\_\_\_\_  
RECRUIT

\_\_\_\_\_  
SERGEANT

\_\_\_\_\_  
FTO COORDINATOR

(FORM 4-5)

**TEAGUE POLICE DEPARTMENT  
MONTHLY / END OF PROBATION  
OBSERVATION REPORT  
\_\_\_\_\_  
THROUGH \_\_\_\_\_**

RECRUIT \_\_\_\_\_ FTO \_\_\_\_\_ SHIFT \_\_\_\_\_ DATE \_\_\_\_\_

RATING INSTRUCTIONS: Rate observed behavior on the scale below using the numerical value definitions contained in the standardized evaluation guidelines. You must comment on the most and least acceptable performance of the day. Although specific comments are required for all ratings of "1" or "6" and above, you are encouraged to comment on any behavior you wish. Use category numbers to reference your narrative comments. Check the "NO" box if a category is not observed.

Assignment or Reason for No Evaluation: \_\_\_\_\_

NOT ACCEPTABLE  
BY FT PROGRAM  
STANDARDS

MINIMUM  
ACCEPTABLE  
LEVEL

SUPERIOR BY  
FT PROGRAM  
STANDARDS

1 2 3 4 5 6 7

**PERFORMANCE TASKS**

**NO**

1 Self-Initiated Field Activity	1	2	3	4	5	6	7	
2 Officer Safety	1	2	3	4	5	6	7	
3 Report Writing & Routine Forms	1	2	3	4	5	6	7	
4 Investigative Skill	1	2	3	4	5	6	7	
5 Problem Solving / Decision Making	1	2	3	4	5	6	7	
6 Department Policies / Procedures	1	2	3	4	5	6	7	
7 Acceptance of Feedback	1	2	3	4	5	6	7	
8 Attitude Toward Police Work	1	2	3	4	5	6	7	
9 Relationship with Public in General	1	2	3	4	5	6	7	
10 General Appearance	1	2	3	4	5	6	7	

(FORM 4-6)

**NARRATIVE COMMENTS**

Additional Comments

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Remedial Training Taken To Correct Deficiencies

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

PROBATIONARY OFFICER \_\_\_\_\_

ASSIGNED FTO \_\_\_\_\_

-----  
EVALUATION REVIEWS

(SERGEANT) WATCH COMMANDER: \_\_\_\_\_

Chief of Police: \_\_\_\_\_

(FORM 4-7)

***RECRUIT PERFORMANCE DOCUMENTATION***

SCALE VALUE APPLICATION

Perhaps the most difficult task facing the rater is the application of a numerical rating that represents the behavior he is evaluating. The rater's dilemma usually involves his rating philosophy versus another's and the question of whom is right. The following explanations should clarify the issues and ease the concerns of the rater and the person being rated.

We use a rating scale, under this program, of "1 to 7". While this may seem to be rather broad, there is a specific reason for its use, over a "1 to 5" scale. First, under the "1 to 7", it is apparent that a "4" is the median range score. Therefore, we must define a "4" as a base to work from. A "4", under this program, is defined as the "minimal acceptable level of performance." In other words, for a specific task, an officer can perform and complete the function independently in an acceptable manner. Notice the key word here is "independently." The FTO must realize that any hints or guidance given the recruit means the recruit did not complete the task "independently", no matter how successful he was. During the initial stages of training, the FTO must show the recruit how to do it and then let the recruit do it. But if our ultimate goal is for the recruit to work alone, then our "cut-off" grade must be "Is the recruit capable of taking this specific task and completing it with no assistance?"

If we understand the definition of a "4", then the next step is to define the two extremes of performance. A "1" is easily defined since it denotes a clear inability to perform the task. A "1" therefore, indicates a "performance not acceptable by program standards as set out in the Standardized Evaluation Guidelines." Any one or a combination of these unacceptable performance definitions, should result in the recruit being assigned a grade of "1."

At the opposite end of the scale is an individual's ability to perform at the superior or exceptional level. While the grade of "7" is the most agreeable to use, it is also the most easily abused. In defining a grade of "7", or superior performance, the FTO must note that in most of the definitions, the word "always" or "all" the time is used. The FTO must ask "has the recruit performed this task flawlessly and with absolutely NO assistance during this rating period?"

In most cases where the grade of "7" is misused, it is because the FTO confuses "superior performance" with a "superior attitude." Keep in mind "Attitude toward Police Work" is a separate category and can give credit to the recruit when it is deserved. It should be noted that few officers are capable of "7" performance, but this should not be viewed as a negative aspect of the program. Instead, the FTO should view the "7" as a goal for



the recruit to strive for and attempt to improve. A "7" should be given to the exceptional recruit, for exceptional performance.

Now that the FTO understands the extreme of the rating scale and our minimal acceptable levels that do not fall into any of the above three categories. As noted above, we utilized a scale of "1 to 7" instead of "1 to 5." The primary reason being that the grades "2 and 3" and "5 and 6" give us much more flexibility in defining "performance capabilities." Under a "1 to 5" scale, if a recruit is not performing at the minimum acceptable level (a "3"), but the recruit's performance is clearly not unacceptable (a "1"), then the only grade left is a "2". However, a valid question for review is, "Is the recruit's performance capability closer to minimum or unacceptable levels?". Under a "1 to 7" scale, a "3", while not meeting the minimum standards, is very close or capable of, reaching them. At the same time, a "2", while not meeting unacceptable standards, is very close or capable of, reaching them. At the same time, a "2", while not meeting unacceptable standards, is very close to becoming so if this level of performance continues. At the opposite end of the scale, it should be clear how to apply the grade of "5 and 6." In applying a grade of "5", the FTO indicates that while the recruit's current performance capabilities are above minimum standards, the recruit is closer to minimum standards than superior standards. Obviously, a grade of "6" indicates that the recruit is closer to superior than minimum standards.

In scale value application, the first principle that must be accepted by all is that each of us has different perceptions on nearly everything in the life experience. While a standardization of ratings is an acute necessity, an attempt to standardize perceptions is doomed to failure at the start. For example, FTO "A", based on prior negative experience of his own, sees a recruit's exposure of his weapon to a suspect as worth a "1" rating (Officer Safety) while FTO "B" may see the same behavior as worth a "3". Should the recruit or we really be concerned? Our answer is "No!" as long as both officers see the performance as "Unacceptable" under the guideline quoted.

A lack of standardization ensues when one FTO sees the performance of an Unacceptable (Scale values 1, 2, or 3) and the other sees the same behavior as "Acceptable," (scale values 4, 5, 6, or 7). In summary then, we have no difficulty accepting differences in officers' perceptions unless these perceptual differences vary between Unacceptable and Acceptable ratings for the same behavior.

The second principle that is important to grasp is the value assigned to performance wherein remedial efforts have been undertaken and the recruit

is not responding to training. A trainee who performs at a less than acceptable level might be assigned 1, 2, or 3 for that task. The FTO is under an obligation to remediate the mistake and assessing the recruit's performance when he has the opportunity to do so. If the FTO has utilized retraining procedures and the recruit continues to fail, a reduction in scale value might seem initially, to be the appropriate step. However, if the recruit's performance has remained essentially the same, (while admittedly below acceptable standards), we should document that the recruit is NOT RESPONDING TO TRAINING (N.R.T.). The N.R.T. section of the Daily Observation Report form allows the FTO to report continued failure and the failure on the part of the recruit to improve, all the while maintaining the integrity of the rating first given.

An N.R.T. is an indication, then, of a problem that has occurred in the past; that has been the object of appropriate remedial effort; and the remedial effort has not produced the desired result. A rating of N.R.T. might be likened to waiving a "red flag" in that the recruit is in danger of failing the Field Training Program unless performance improves in that area. (See Chapter 7, "Remediation").

In summary, do not evaluate the recruit against the average recruit or against a recruit in the same class or with the same amount of experience. Instead, evaluate the recruit based on his ability to function and perform the task in an acceptable and independent manner.

### Narrative Support for Performance Scale

While the Performance Scale defines overall capabilities of the recruit, different circumstances may well mitigate or enhance the specific grade. Therefore, the FTO's specific evaluation of the day's performance is so critical. A narrative overview supports and clarifies the FTO's numerical evaluation.

Under program guidelines, narrative comments are required for grades of "1, 6, 7, and NRT." It should be noted, however, that comments on any behavioral aspects of the recruit are encouraged. The FTO is also required to comment on the most acceptable performance(s) of the day (phase) and improvements needed for the day (phase).

During Phase I, it is expected that the recruit will make more mistakes and his performance will be less polished. Therefore, it is reasonable for the recruit to earn more "2's" and "3's" during this period. Obviously, a grade of

"1", while significant, would not be as critical in the category of Orientation or Self-initiated Field Activity as a grade of "1" in the category of Officer Safety would indicate. It is important for the FTO to realize that narrative support for the overall evaluation should not only clarify positive and negative performance, but also should indicate steps necessary to improve.

During Phase II, grades of "2 and 3", while not requiring comments, begin to indicate significant weaknesses. The FTO is encouraged to document these weaknesses and to give the recruit, specific steps to improve. The FTO at this point must also give serious consideration to Intensive Remedial Training in areas where no improvement is seen. Documented support of the numerical evaluation makes this step much easier to justify. By the end of Phase II, the recruit should have all "4" s before being passed on to Phase III.

A thorough narrative should include, but not be limited to, the following components: Specific, concise sentences, call for service numbers, ticket numbers, locations and times. If the narrative is involved, the FTO should make a brief statement of strengths and weaknesses in the indicated sections and then expand on the needed areas under additional comments. It is suggested that the FTO indicate the specific performance category number(s) before each specific narrative statement; in other words, make it easy for the reviewer to relate the narrative comments back to the specific grades on the observation reports. In addition, this ensures that the FTO's narrative comments are consistent with the performance grades given.

In summary, the narrative component of the Observation Report is a critical aspect that compliments and supplements the performance grades. The program does not expect "great author" capabilities, just clear, factual support for the grades given the recruit.

### ***FIELD TRAINING PROGRAM CRITIQUE***

The purpose of the Field Training Program Critique is to solicit from the new officer information, which may be used to improve the Field Training Program, (See Forms 4-8 and 4-9). It consists of a series of program-related questions, and a comment page for inclusion of any additional information or comments the officer may wish to make.

The critique will be completed during an interview with the Field Training Supervisor. The interview will be held within 14 days after successful completion of the full sixteen-week Field Training Program.

During the interview, the Field Training Supervisor will note and forward to the immediate supervisor any information regarding alleged improprieties by a Field Training Officer. It will be the responsibility of the FTO's shift Supervisor to take any action this information deems necessary.

The Field Training Supervisor will analyze the completed critiques. Serious consideration will be given to comments, which will assist them in improving the Field Training Program.

A copy of the completed critique will be maintained in the file of each Field Training Officer to which the recruit was assigned. Field Training Officers may review the critiques in the presence of the Field Training Supervisor.

**TEAGUE POLICE DEPARTMENT  
FIELD TRAINING AND EVALUATION PROGRAM**

DATE: \_\_\_\_\_

NAME: \_\_\_\_\_ BADGE: \_\_\_\_\_

1. Is there anything in the FTO Program that you were not taught that you feel you should have been?

---

---

---

2. Can the department do anything different to prepare a recruit officer for entry into the Field Training Program? BE SPECIFIC:

---

---

---

3. Do you have any suggestions for improvement in the FTO Program?

---

---

---

4. Were you ever placed in an element with other than a Field Training Officer? If so, which rotation?

---

---

---

5. Do you feel that after 16 weeks of Field Training, you can competently perform the duties of a Teague Police Officer, or do you feel you needed additional time?

---

---

---

6. How do you feel about your chosen career as a Teague Police Officer?

---

---

---

PLEASE CONTINUE OR ADD ADDITIONAL NARRATIVE ON THE "ADDITIONAL COMMENTS" SHEET.

(FORM 4-8)

ADDITIONAL COMMENTS:

---

---

---

---

---

---

---



# **CHAPTER 5**

## **STANDARD EVALUATION GUIDELINES**

# **TEAGUE POLICE DEPARTMENT**

## **STANDARDIZED EVALUATION GUIDELINES**

### **(1) DRIVING SKILLS:      NORMAL CONDITIONS**

- |                 |   |
|-----------------|---|
| 1. Unacceptable | Continually violates Traffic Code (speed, traffic signals, etc.); involved in chargeable accident or vehicle damage; lacks dexterity and coordination during vehicle operation. |
| 4. Acceptable   | Ability to maintain control of vehicle while being alert to activity outside of vehicle. Practices good defensive driving techniques.   |
| 7. Superior:    | Sets good example of lawful, courteous driving while exhibiting good manipulative skill required of police officer (i.e., operate Radio, utilize hot sheet).                    |

### **(2) DRIVING SKILLS:      STRESS CONDITIONS**

- |                  |   |
|------------------|---|
| 1. Unacceptable: | Involved in accident(s). Unnecessary Code 3. Over uses red lights and siren. Excessive and unnecessary speed. Fails to slow for intersections and loses control on corners. |
| 4. Acceptable:   | Maintains control of vehicle. Evaluates driving situation and reacts properly. (i.e., proper speed for conditions)  |
| 7. Superior:     | High degree of reflex ability and competence in driving skills.   |

### **(3) ORIENTATION/RESPONSE TIME TO CALLS:**

- |                  |   |
|------------------|---|
| 1. Unacceptable: | Becomes disoriented when responding to stressful situations. Is unable to relate his/her location to his/her destination. Is unable to use a map under stress. Is unable to determine directions of the compass during stressful tactical situations. |
| 4. Acceptable:   | Reasonably aware of his/her location. Can utilize a map effectively under stressful conditions.   |



Demonstrates good sense of direction in tactical situation.

7. Superior: Always responds quickly to stressful calls by the most appropriate route. Does not have to refer to a map. Rarely disoriented during tactical situations.

**(4) FIELD PERFORMANCE: STRESS CONDITIONS**

Evaluates the Recruit's ability to perform in moderate and high stress situations.

1. Unacceptable: Becomes emotional, is panic-stricken, can't function, holds back, loses temper or displays cowardice. Over reacts.
4. Acceptable: Maintains calm and self-control in most situations, determines proper course of action and takes it. Does not allow the situation to further deteriorate.
7. Superior: Maintains calm and self-control even in the most extreme situations. Quickly restores control in the situation and takes command. Determines best course of action and takes it.

**(5) SELF-INITIATED FIELD ACTIVITY/OBSERVATION SKILLS:**

1. Unacceptable: Fails to observe or avoids activity. Does not follow up on situations requiring police attention, rationalizes suspicious circumstances and does not investigate.
4. Acceptable: Observes, recognizes, and identifies suspected criminal activity or situations requiring police attentions. Makes cases and arrests from routine activity, while on vehicle or foot patrol.
7. Superior: Catalogs, maintains, and uses information issued at briefings and other sources for reasonable cause to stop vehicles and persons, and makes subsequent good quality arrests. Provides good police service by observing and recognizing non-criminal situations and helping, either while on vehicle or foot patrol.

**(6) OFFICER SAFETY:**

Evaluates the Recruit's ability to perform police tasks without injuring self or others exposing self or others to unnecessary danger/risk.

- 1. Unacceptable: Fails to follow accepted safety procedures or to exercise officer safety, i.e.:
  - A) Exposes weapons to suspect (baton, handgun, etc.).
  - B) Fails to keep gun hand free during enforcement situations.
  - C) Stands in front of violator's car door.
  - D) Fails to control suspect's movement.
  - E) Does not keep suspect/violator in sight.
  - F) Fails to use illumination when necessary or uses it improperly.
  - G) Fails to advise dispatcher when leaving police vehicle.
  - H) Fails to maintain good physical condition.
  - I) Fails to utilize or maintain personal safety equipment.
  - J) Does not anticipate potentially dangerous situations.
  - K) Stands too close to passing vehicular traffic.
  - L) Is careless with gun and other weapons.
  - M) Stands in front of doors when knocking.
  - N) Makes poor choice of which weapon to use and when to use it.
  - O) Fails to cover other officers.
  - P) Stands between police and violator's vehicle on car stop.
  - Q) Fails to search police vehicle prior to duty and after transporting suspect.
  
- 4. Acceptable: Follows accepted safety procedures. Understands and applies them.
  
- 7. Superior: Always works safely. Foresees dangerous situations and prepares for them. Keeps partner informed and determines the best position for self and partner. Is not overconfident. Is in good physical condition.

**(7) CONTROL OF CONFLICT: VERBAL SKILLS**

- 1. Unacceptable: Improper voice inflection; i.e., too soft, too loud, confused voice command or indecisive; poor officer bearing.
  
- 4. Acceptable: Speaks with authority in a calm, clear voice.

7. Superior: Always gives appearance of complete command through voice tone and bearing.

**(8) CONTROL OF CONFLICT: PHYSICAL SKILLS**

1. Unacceptable: Physically weak or uses too little or too much force for given situation. Unable to use proper restraining holds.
4. Acceptable: Maintains control without excessive force. Properly applies restraining holds.
7. Superior: Always prepared to use necessary force. Excellent knowledge of and shows the ability to use restraining holds.

**(9) RADIO: COMPREHENSION/USAGE**

1. Unacceptable: Misinterprets communication codes, definitions or fails to use radio in accordance with set policy; fails or refuses to improve. Repeatedly misses his/her call sign and is unaware of radio traffic on adjoining beats. Frequently must ask Dispatcher to repeat transmission or does not comprehend message.
4. Acceptable: Copies most radio transmission directed to him/her and is generally aware of adjoining beat traffic. Uses proper procedures with clear, concise, and complete transmissions. Has good working knowledge of radio codes.
7. Superior: Transmits clearly, calmly, concisely, and completely in even the most stressful situations. Transmissions are well thought out and do not have to be repeated. Uses communication codes with ease in all receiving and sending situations.

**(10) ROUTINE FORMS: ACCURACY/COMPLETENESS**

Evaluates Recruit's ability to properly utilize departmental forms necessary to job accomplishment.

1. Unacceptable: Is unaware that a form must be completed and/or is unable to complete proper form for the given situation. Forms are incomplete, inaccurate, or improperly used.

4. Acceptable: Knows the commonly used forms and understands their use. Completes them with reasonable accuracy and thoroughness.
7. Superior: Consistently makes accurate form selection and rapidly completes detailed forms without assistance. Displays high degree of accuracy.

## **(11) REPORT WRITING: ORGANIZATION/DETAIL**

Evaluates the Recruit's ability to prepare reports that accurately reflect the situation and in a detailed, organized manner.

1. Unacceptable: Unable to organize information and to reduce it to writing. Leaves out pertinent details in report. Report is inaccurate. Reports are illegible. Reports contain excessive number of misspelled words. Sentence structure or word usage is improper or incomplete.
4. Acceptable: Completes reports, organizing information in a logical manner. Reports contain the required information and details. Reports are legible, and grammar is at an acceptable level. Spelling is acceptable, and errors are rare. Errors, if present, do not impair an understanding of the report.
7. Superior: Reports are a complete and detailed accounting of events from beginning to end, written and organized so that any reader understands what occurred. Reports are very neat and legible. Contain no spelling or grammar errors.

## **(12) REPORT WRITING: APPROPRIATE TIME USED**

Evaluates the Recruit's efficiency relative to the amount of time taken to write a report.

1. Unacceptable: Requires an excessive amount of time to complete a report. Takes three or more times the amount of time a non-probationary officer would take to complete the report.
4. Acceptable: Completes reports within a reasonable amount of time.
7. Superior: Completes reports very quickly, as quickly as that of a skilled, veteran officer does.



procedure.

1. Unacceptable: Fails to use proper questioning techniques. Does not elicit and/or record available information. Does not establish appropriate rapport with subject and/or does not control interrogation of suspect. Fails to give Miranda warning.
4. Acceptable: Generally, uses proper questioning techniques. Elicits most available information and records it. Establishes proper rapport with most victims/witnesses. Controls the interrogation of most suspects and generally conducts a proper Miranda Warning.
7. Superior: Always uses proper questioning techniques. Establishes rapport with all victims/witnesses. Controls the interrogation of even the most difficult suspects. Conducts successful interrogations. Always gives a proper Miranda warning.

**(16) PROBLEM SOLVING/DECISION MAKING:**

1. Unacceptable: Acts without thought or is indecisive. Relies on others to make his/her decisions.
4. Acceptable: Is able to reason out problems and relate what he/she was taught. Has good perception and ability to make his/her own decisions.
7. Superior: Excellent ability to foresee problems and arrive at sound decisions.

**(17) DEPARTMENTAL POLICIES/PROCEDURES:**

Evaluation of the Recruit's knowledge of the department's policies and procedures and the ability to apply this knowledge under field conditions:

1. Unacceptable: When tested verbally or in writing, the Probationary Officer scores 20% or less. When applied in the field, the officer shows little or no knowledge of departmental policy or fails to use the appropriate procedure when it applies.
4. Acceptable: When tested verbally or in writing, the Probationary Officer scores at least 70%. When

applied in the field, the officer shows a familiarity with the most commonly used policies and procedures.

7. Superior: When tested verbally or in writing, the Probationary Officer scores 100%. When applied in the field, the officer is familiar with all the policies and procedures and uses the appropriate one when needed.

**(18) PENAL CODE, CODE OF CRIMINAL PROCEDURE, AND CITY ORDINANCES:**

Evaluation of the Recruit's knowledge of the criminal statutes, and ability to apply that knowledge in the field:

1. Unacceptable: When tested verbally or in writing, the recruit scores 20% or less. When applied in the field, the officer does not know the basic elements of a crime when encountered or makes mistakes that would indicate lack of that knowledge necessary to conduct a successful investigation and write a good report.
4. Acceptable: When tested verbally or in writing the recruit scores at least 70%. When applied in the field, the officer recognizes commonly encountered criminal offenses and knows what actions are necessary to make the case capable of successful prosecution.
7. Superior: When tested verbally or in writing the recruit scores 100%. When applied in the field, the officer displays an outstanding knowledge of the codes and applies this knowledge while in both normal and unusual criminal situations.

**(19) VEHICLE CODE:**

Evaluation of the Recruit's knowledge and ability to apply the traffic laws of the State to field enforcement:

1. Unacceptable: When tested verbally or in writing, the Probationary Officer scores 20% or less. When applied in the field, the officer shows a poor working knowledge of the traffic code and its practical application.

4. Acceptable: When tested verbally or in writing, the Probationary Officer scores at least 70%. When applied in the field, the officer shows a good working knowledge of the traffic laws and can apply the correct statute to the situation.
7. Superior: When tested verbally or in writing, the Probationary Officer scores 100%. When applied in the field, the officer demonstrates an unusually acute knowledge of even the most seldom used vehicle code statutes.

**(20) ACCEPTANCE OF FEEDBACK/FOLLOWING INSTRUCTIONS:**

Evaluation of the Recruit's acceptance of constructive criticism and instruction and how the officer uses the information and instructions provided to improve performance.

1. Unacceptable: Rationalizes mistakes, denies that errors were made, is argumentative, refuses to do or does not attempt to make corrections. Considers criticism a personal attack.
4. Acceptable: Accepts criticism and instructions in a positive manner and applies the information to make correction in performance.
7. Superior: Actively solicits criticism and instructions in order to improve performance. Instructions do not have to be repeated.

**(21) ATTITUDE TOWARD POLICE WORK:**

Evaluation of the Recruit's attitude toward new career in terms of personal motivation, goals, acceptance or responsibility and career objectives:

1. Unacceptable: Sees career as only a job; uses position to boost ego; abuses authority; shows little dedication to the principles of professionalism.
4. Acceptable: Demonstrates an active interest in the new career and takes the new responsibility seriously.
7. Superior: Utilizes off-duty time to further professional knowledge and expertise; solicits





1. Unacceptable: Patronizes FTO/Superiors/peers or is antagonistic toward them. Gossips. Is insubordinate, argumentative, and sarcastic. Resists instructions. Considers self-superior. Belittles others. Is not a "team" player.
4. Acceptable: Adheres to the chain of command and accepts role in the organization. Good peer and FTO relationships and is accepted as a group member. Shows proper respect to supervisors.
7. Superior: Is at ease in contact with all, including superiors. Understands superiors' responsibilities, respects and supports their position. Peer group leader. Actively assists others.

**(25) GENERAL APPEARANCE:**

Evaluates physical appearance, dress, and demeanor.

1. Unacceptable: Overweight, dirty shoes or wrinkled uniform. Uniform fits poorly or is improperly worn. Hair in need of grooming and/or in violation of department regulation. Dirty weapon, equipment. Equipment missing or inoperative. Offensive body odor or breath.
4. Acceptable: Uniform neat, clean. Uniform fits and is worn properly. Weapon, leather, equipment is clean and operative. Hair within regulations, shoes are shined.
7. Superior: Uniform neat, clean, and tailored. Leather and shoes are highly shined. Equipment maintained in excellent condition.

# **CHAPTER 6**

## **REMEDIAL TRAINING**

## **FIELD TRAINING PROGRAM**

### ***REMEDICATION OF PERFORMANCE***

Remedial training is the name given to additional and/or repetitive instruction in an area or areas where skill is weak. Most of this remedial training can be handled on a day-to-day basis by the FTO with the assistance of the sergeant.

FTO's should be cognizant of the usefulness of remedial training and should be quick to provide additional and innovative instruction when needed. The training officer must also realize that there are instructional resources available other than his own teaching talents. With the cooperation of the sergeant, the FTO should, if needed, draw on sources from outside the Department as well as those within, to achieve the desired result, a proficient and knowledgeable recruit. Written tests and homework assignments also should not be forgotten as tools to facilitate remedial training.

The Field Training Program emphasizes four (4) specific steps in training and correcting deficiencies of the recruit. The first obvious step is that the recruit must be given initial - basic instruction, in other words, "show him how to do it." While the FTO is obligated to interact with the recruit as a mature adult, the FTO cannot assume anything and must ensure the recruit has been given reasonable exposure to each task.

The term "reasonable exposure" then becomes the key factor. The FTO must divide each performance task into two (2) categories: Simple tasks and complex tasks. Telling time, work schedules, and bringing the appropriate equipment to work are examples of simple tasks. Major felony investigations, traffic stops, and domestic disturbances are examples of complex tasks. Obviously the FTO will give less reasonable exposure to a simple task and more to a complex task. At this point, only the performance grade and supporting narrative will be utilized.

Once the FTO has given the recruit reasonable exposure to the task and the recruit still has trouble in performing the task in an acceptable manner, the FTO must move to the second training step. "Basic Daily Remediation" of a weak skill or performance ensures that the recruit has had the deficiency brought to his attention. This remediation may range from several minutes of verbal counseling, to a specific homework assignment, or

to several hours of special assignment working on the deficiency. The performance grade will still be noted, and a specific supporting narrative now becomes essential.

In addition, the total number of minutes (or hours) provided for the specific training should be entered in the space provided at the bottom of the D.O.R. Also, the FTO must explain the type of remedial training in the "Comments" section. This documentation should be labeled "Remedial Training," describe the specific problem, define what the solution to the deficiency is, and what specific action was taken. Reasonable "Initial Training," based on task difficulty, is a prerequisite for Basic Daily Remediation.

In some cases, the recruit will not respond to this initial remediation in a manner that will bring his performance up to an acceptable level. When the FTO believes that the recruit has had a reasonable amount of Initial and Basic Remedial Training, based on the task difficulty, and still is not performing at a satisfactory level, the FTO will move to the third step of remediation. The "Not Responding to Training" (NRT) block, as noted earlier, is an indication that the problem has occurred in the past; that is, has been the object of appropriate remedial effort; and the remedial effort has not produced the desired results. Remediation efforts in this step will remain somewhat like that in Basic Daily Remediation. These efforts will now become more specific and intensified. However, the FTO will document this failure to respond to Basic Remediation by marking the appropriate "NRT" box in the D.O.R. form. The FTO will also continue to record the appropriate performance grade, document the recruit's performance in the narrative section, and note the number of minutes (or hours) of remedial training required. Reasonable Basic Daily Remediation, based on task difficulty, is a prerequisite for checking the "Not Responding to Training" block.

Up to this point, the remediation of the recruit's deficiencies has been done as a part of the officer's normal training progression. In some cases, however, a deficiency is so pronounced that the recruit must be removed from the program so that specific attention can be given to the weakness. A pattern of failures to respond to remedial training (NRT) is a prerequisite for consideration of "Intensive Remedial Training."

Whenever the need to remove the recruit from his normal training schedule for intensive remediation is recognized, a written "Request for Intensive

Remedial Training" will be made to be FTO Supervisor through the chain of command, (See Form 6-1 and 6-2). When the recruit completes their intensive remedial training program, he will be placed back into the program schedule for completion of field training.

The FTO Supervisor will, therefore, be required to extend the recruit's training schedule by the number of days/weeks in the remedial program.

FTO's, FTO Team Supervisors, and the FTO Supervisor must answer yes to all the following questions before injecting a recruit into an intensive remedial program:

1. Is there a specific, identifiable problem?
2. Is the recruit's deficiency one that can be corrected or cured with additional instruction? (Some deficiencies are character traits or learning disabilities that cannot be corrected and termination is the only option).
3. Can we hope to correct this deficiency or teach this skill within a reasonable time period, one to four weeks?
4. Have there been basic daily remedial training and NRT's without adequate improvements?

To facilitate intensive remedial training, the recruit may be assigned to any watch and FTO that will best accomplish the goal. The FTO to whom the recruit is assigned may or may not have previously trained him. It is suggested, however, that consideration be given to assigning the recruit to an FTO that is not in the officer's normal rotation. This allows for a separate opinion of the recruit's performance and capabilities. In addition, the recruit may be assigned outside the Patrol Division, i.e., outside tutoring etc. During an Intensive Remedial Training Program, the recruit will continue to receive D.O.R.'s from the FTO and sergeant. The FTO will indicate this status by noting the appropriate number in the "Phase" block and noting "I.R.T." in the week block. Should this Intensive Remedial Training be for more than one (1) week, note it as such by "I.R.T." - Wk 1", "I.R.T. - Wk 2", etc.

If the recruit remains on the same watch or is assigned outside the Patrol Division for the I.R.T., then the sergeant's Weekly Report and review of each week's D.O.R.'s will be done by the supervisor requesting the training. Should the recruit be assigned to another watch in the same division, the

FTO supervisor the recruit is assigned to, will be responsible for the above report and review.

Generally, the recruit will not pass or fail Intensive Remediation. The purpose of this training is to correct and resolve a problem. It is still the responsibility of the regularly assigned FTO to evaluate the recruit's performance in the normal training process.

Only if an excessive safety deficiency or major violation of policy comes to light, would the recruit be considered for termination during Intensive Remedial Training.

In summary, this program is built on a foundation of training and remediating recruit performance. The FTO is obligated to remediate deficiencies whenever possible. The training officer should consider the monetary and time investment in getting the recruit to this point. The Field Training program recognizes that in some cases, a personality trait or character flaw may exist that will have a negative impact on the recruit's performance and cannot be remediated. In some very isolated cases, remediation of the recruit may not be feasible beyond the "Not Responding to Training" stage. However, in the vast majority of situation, application of sound professional principles and thorough documentation of the recruit's performance will accomplish our goals as an instructor and teacher.

## ***REMEDIAL TRAINING TECHNIQUES***

### **INTRODUCTION**

Clarifying and correcting a recruit's *deficiencies* is probably the most critical and yet most challenging aspect of an FTO's responsibility. As previously noted in Chapter 5, this training program is broken up into four (4) phases. Three (3) of the phases are for training purposes. The final phase is for evaluation purposes only.

While the FTO will have overall goals for training of the recruit, each phase should also have specific goals to achieve. During Phase I, the FTO should attempt to initiate the recruit to basic police functions. As a result of this initial exposure, the FTO should, by the end of this phase, be able to identify specific strengths and weaknesses of the recruit.

The Phase II FTO should review the Phase I accomplishments and deficiencies. The primary goal of the Phase II and III FTOs should be to correct all the routine recruit deficiencies that are easily identifiable. The most common deficiencies a recruit will exhibit are in the areas of Geography, Report Writing, Decision Making, Public Contact-Interview Skills, and Radio Usage. Also, Phase III should be utilized for "Polishing and Refining" the existing skills of the recruit. Any significant deficiencies should be completely resolved, generally, by the middle of this phase. Should the recruit need to be placed in Intensive Remedial Training, this will allow sufficient time to correct and then appraise the performance. The last few weeks of this phase should be used to acclimate the recruit to work as a solo officer. This will smooth the transition into Phase IV.

### **TYPICAL TRAINING PROBLEMS**

Most veteran training officers will identify four primary areas as being stumbling blocks to most recruits. Below are some suggested approaches to be utilized in correcting a recruit's unacceptable performance.

### **GEOGRAPHY AND ORIENTATION**

The most common weakness a recruit will exhibit will be in this area. The FTO must be reasonable and realistic in his expectations of the recruit. Initially, the recruit should be expected to know where he is a majority of the time, know where he is going to, and be able to use a map to get from "Point



A to Point B." A recruit cannot possibly know the city as well as his FTO does. The FTO's primary responsibility is to teach principles and fundamentals of geography and orientation skills. The primary question then, is not whether the recruit took the fastest route, but whether the recruit took a route that got you there in a reasonable amount of time, based on his experience and capabilities.

A Recruit Officer should be expected to know at least the following fundamentals:

1. How to utilize compass directions.
2. Base lines for dividing north/south and east/west block numbers.
3. Major north/south and east/west streets.
4. Block numbers at major intersections.
5. How to read and use a map.

Should the recruit have trouble, the following may be helpful in improving their performance:

1. Use of major landmarks.
2. Use of the sun.
3. Memorizing major streets.
4. Homework assignments using blank maps, with major streets, noting block numbers at intersections.
5. Have the recruit highlight street names and cross reference in the index section of the map for streets in your area.
6. Highlight major streets initially, then mark each street as the recruit encounters them on call. Also consider having the recruit highlight street names on a map, as a homework assignment.
7. Have the recruit verbally drive you from "Point A to Point B."
8. Make practice runs by giving the recruit several locations and having

him drive you to them.

9. The recruit should be allowed to drive at least half of each shift. This allows him to not only interact with orientation skills, but stress and observation skills. The only exception to this should be during the first few weeks of training or if specific problems exist and there is documentation to support not driving.
10. Written and verbal tests covering material learned to date.

The above list is obviously not all-inclusive but represents some tried and proven techniques. Any approach that the FTO can use that works is valid, however.

### REPORT WRITING

An individual's ability to relate in writing, what he has done, observed, or needs, is probably the most important attribute of a police officer. This skill is, in most cases, also the most difficult to remediate where a major deficiency exists.

If the FTO notes an obvious deficiency in this area, the FTO should review the recruit's training to date and then establish answers to the following question:

1. Has the recruit received reasonable exposure and hands on application of the skills needed?
2. Does the recruit have any obvious learning disabilities?
3. Is the recruit having difficulty applying laws and policies to the situation, or can the recruit simply not express himself in writing?
4. Does the problem appear to relate to an organizational deficiency or educational deficiency?

In other words, if the recruit cannot "spell", do they know that fact? Is the recruit too lazy to look the word up, or does he not realize the difference? The former can be remediated, the latter will be difficult to deal with.

Specific documented answers to the above questions should at least give the FTO a direction to work from. The FTO program recognizes that some

deficiencies in this area may well be beyond the training and expertise of the FTO. In some cases, resources outside the Department may be sufficient to resolve the problem. In a few isolated situations, however, we must realize that the problem cannot be resolved in a reasonable and timely manner.

If the recruit does experience problems in Report Writing, the following may be helpful in improving their performance:

1. Always have the recruit carry a pocket dictionary.
2. Have them write all reports.
3. Assign the recruit to the Records Section for an appropriate period to observe and review the composition of incoming reports.
4. Have the recruit "verbalize" the incident, with what action(s) he took or recommends taking, before ever attempting to reduce the incident to writing. Keep in mind that if the recruit does not understand what transpired mentally; he will not be capable of relating the incident in writing.
5. Have the recruit establish a consistent pattern of obtaining information in a specific chronological order.
6. Does the recruit understand, and can they apply the concept of "Who, What, When, Where, Why, and How?" (I.e., Who did What to Whom? Who saw it happen? When, Where, Why, and How did it happen?)
7. Make sure the recruit understands the relationship between the complainant and suspect(s). This item may not prove the case but may clarify the incident.
8. When a problem in this area begins to surface, make copies of some of the initial report efforts. Include on those copies appropriate corrections, indicating the amount of time it took to produce an acceptable report. If a serious deficiency exists, begin including a more comprehensive sample in your documentation, with appropriate corrections. This method helps clearly establish a pattern of improvement or digression.

This list is not all-inclusive but does address some proven techniques. The FTO is encouraged to try any method that gets the job done and remains

within the policies of the program and department.

## DECISION MAKING

As noted earlier, one of the major goals for the FTO to meet is to teach the recruit how to make decisions. This is a critical skill for any police officer to possess. Yet it is a skill that cannot be learned by reading a book or watching a video presentation. Decision making must be learned, for the most part, the same way you learned to ride a bicycle, "You get on and you fall off a few times."

The most difficult task for the FTO will be to "just let the recruit do it." Given the FTO's experience level he can deal with most situations in an expeditious fashion, however this does little to enhance the recruit's skills. The FTO should hold the recruit responsible for decisions that progressively become more complex, relative to the recruit's experience.

The most important aspect of "Decision Making" for an FTO to teach the recruit is, "Why did you make that decision and what policies, or laws did you use to make it?" The FTO must realize that the recruit may well take the appropriate action, but did he do it for the appropriate reason? The FTO should utilize every possible opportunity to interact with the recruit and assess the trainee's ability to apply the correct theory, to a realistic situation, in a practical manner. This may well involve complimenting the recruit for a job well done, but asking in a low-key manner, "Why did you decide to handle it that way?" In some instances, the recruit may just note that "it was the right thing to do." Make sure that each decision and each action is based on clear policy or legal guidelines. Also, ensure that the recruit knows how far he can vary from these guidelines and why.

Remediation of this skill is much more difficult since you are dealing with a performance that is based, in part, on pre-learned behavior. Depending on the nature of the deficiency, the FTO must first be sure to document and define the weakness. Initial remediation will center on redefining the recruit's responsibilities and clarifying relevant policies and regulations. It may be wise for the FTO to volunteer for calls, when possible, that relate the recruit's deficiency. For instance, volunteering for family violence calls where the recruit is having problems taking control and deciding what to do in a stress situation.

More specific remediation may require special assignment time in which the recruit will respond only to the type calls or incidents that give him a specific

opportunity to practice these skills. If the deficiency shows a lack of reasonable improvement, and appropriate remediation has been exercised and documented, then the recruit may need to move into Intensive Remediation.

During this specialized training, the recruit should, when possible, be placed with a different FTO. An FTO should be selected that has a background in this type problem and the maturity to make some critical judgment decisions, relevant to the recruit. In assigning the recruit to this remediation, a watch and beat with sufficient activity may also be a consideration.

As noted earlier, the recruit will not pass or fail this remediation. The recruit should be given the opportunity to return to his regularly assigned FTO and demonstrate whether he can perform at an acceptable level. The important factor in utilizing another FTO for Intensive Remediation is the additional opinion and appraisal of the recruit's performance and capabilities.

Also noted earlier, decision-making skills are a critical and required attribute for a police officer to possess. A major deficiency here may well affect the recruit's career potential. This area is also probably the hardest to evaluate since the FTO's communication, perception, and interaction skills will have a bearing on the recruit's learning and capability. The FTO should remember that specific and detailed documentation is mandatory in this category.

## RADIO USAGE

Police radio communication skills seem to be a consistent weakness for most recruits, at least during the early stages of training. Most deficiencies revolve around the following:

1. An inability to acknowledge and comprehend dispatcher's comments, as they relate to the recruit's element and elements in the surrounding area.
2. An inability to transmit brief, concise, and logical data to the dispatcher and other field elements.
3. An inability to apply departmental policies as they relate to radio communication skills, i.e., proper data sequence, use of mark-outs, etc.

Remediation of this skill will correspond, at least in part, to the personality

and processing skills of the recruit. The FTO should first be aware that the recruit has a great deal of data and experience to absorb, in a short period of time. The FTO can, generally, carry on a conversation, observe outside activity, drive the patrol vehicle, and still be aware of relevant radio transmissions. The recruit has yet to develop and sharpen this skill. Some recruits will acclimate quickly, others will develop at a slower pace.

If the recruit develops problems in this area, after a reasonable amount of exposure, the FTO should answer the following questions:

1. Has the recruit been shown the proper techniques to use?
2. Has the recruit had the opportunity to practice those techniques and has this been documented?
3. Has the FTO addressed the specific deficiency of the recruit?

The FTO's remediation of this deficiency should include at least some of the following techniques:

1. Have the recruit practice radio transmissions with the FTO during routine patrol.
2. Have the recruit advise the FTO of radio traffic that affects surrounding beats.
3. Ensure the recruit knows to ask the dispatcher to repeat any transmissions not understood.
4. Send the recruit to the Communications Division for an appropriate amount of time. This will allow the recruit to interact personally with the dispatcher and relate to how the data is processed from that end.
5. Have the recruit organize his thoughts before making a transmission. Where possible, say it out loud before transmitting the message.
6. Ensure the recruit knows key phrases and data to note and copy down when interacting with the dispatcher.
7. Have the recruit check suspects, vehicles, and property on the radio.

A deficiency in Radio Usage, while somewhat common, is one area that can

be remediated, in most cases, with some simple techniques and a little extra effort. It is possible that Radio Usage could develop into a major deficiency, but most likely the recruit would be having trouble in other notable areas.

## CONCLUSION

Only a sample of the consistent deficiencies experienced by recruits were addressed in this section. The purpose here was to expose the FTO to "Remediation Progression and Procedures." The reader should have noted at this point that initial training and documentation are the key factors. The FTO can instruct, interact, and counsel with the recruit at length, relative to the displayed deficiency. Without the appropriate documentation, however, the FTO's efforts are for all intents and purposes, meaningless.

**TEAGUE POLICE DEPARTMENT**







# **CHAPTER 7**

## **TERMINATION PROCEDURES**

## **FIELD TRAINING PROGRAM**

### ***CONSIDERATION OF TERMINATION***

The goal of the Field Training Program is to produce a fully trained, competent patrol officer, and the Program expects all recruits to be successful. Unfortunately, some are not and regardless of the efforts by the Program personnel, some do not reach the level of competence required. Recruits sometimes realize their expectations of law enforcement were false ones. Other recruits cannot perform multiple tasks. Still others are unable to deal with the stress present in the job. There are many reasons, but the fact is that some people do not make it, and therefore, must be terminated.

Termination is stressful, not only for the recruit, but for the Program personnel as well. Despite this, in some cases, termination is not only necessary but obligatory. If a recruit is not progressing in the Program and it has been determined that progress to a satisfactory level is not possible, termination is the only logical step.

Field Training Officers often hope to "save" new employees who are failing, and this is laudable but not always fruitful. Personnel should never give up on a recruit who has the slightest chance of success but must be realistic with those who do not. Organizationally, the retention of an employee who is not capable of performing the job would place the Department and the recruit in an untenable position. Not only would liability be ever present, but also such a decision would cost the Department economically and in terms of efficiency. By coming to grips with a recruit's failure, the stress experienced by the recruit will be reduced and the transition to another career will be eased.

The recruit is, of course, subject to the same rules and regulations that govern all Teague Police Officers, and should they violate a criminal statute or Departmental policy, they will be held accountable as prescribed in the policies. Otherwise, recruit terminations will be handled as follows:

### **WHEN TERMINATION MAY OCCUR**

In all cases where possible, the recruit should be given the benefit of training through the first three phases before a termination recommendation is considered. However, the recruit may be terminated at any point in the Program if:

1. He is a threat to his safety or the safety of others; or
2. He repeatedly brings discredit or embarrassment to the Department; or
3. He cannot perform basic tasks necessary to allow him to proceed in the Program.

### ***THE DECISION TO TERMINATE***

Before a decision to terminate is made, some questions must be asked:

1. What are the problems of the recruit?
2. What is causing these problems?
3. What have we done to overcome these problems?
4. How much remediation has been completed?
5. Has there been any improvement after remediation?
6. What are the chances that the recruit will improve in the future?
7. Have we fully documented these problems?

Once the FTO, and FTO Supervisor have reviewed these questions, and they decide that termination is the only feasible option, the Chief will be notified. The Chief of Police will then cause a meeting to be held at which the following personnel are in attendance:

1. All FTO's who have trained the recruit.
2. All FTO Supervisors involved in the recruit's training.

The purpose of this meeting is to discuss the recruit's performance and to ensure that the recruit has been given every chance to succeed. If at the conclusion of this meeting, the consensus is still to discharge the recruit, termination recommendation will be made.

## NOTIFICATION OF THE RECRUIT

As soon as possible after the meeting, the FTO Supervisor will notify the recruit of the impending termination. Although the FTO has been trained to continually keep the recruit informed, it is not the FTO's role to notify the recruit of a termination recommendation.

At the time of the recruit's notification, he should be reassigned from patrol duties or given leave until his discharge. The recruit should not be allowed to perform normal field duties. He is under too much stress and presents a liability to himself, others and the Department.

## ***THE TERMINATION PACKAGE***

The current FTO Sergeant will be responsible for compiling a Termination Package and forwarding it to the Chief of Police. The Termination Package will consist of:

1. A report from each FTO that has trained the recruit,
2. A cover report from the FTO Supervisor,
3. The recruit officer's Police Recruit Guide,
4. A copy of all FTO related reports, and
5. Associated administrative letters and memorandums.

A discussion of each component of the packet may assist in its preparation.

1. The FTO Report: These reports will be in memorandum form and will detail the progress and performance of the recruit. Generally, these memorandums should be entitled, "Field Training Performance of Recruit \_\_\_\_\_." This will allow each FTO to prepare the documentation based on his own perception of performance.

These memorandums may be written in chronological order or category-by-category but must contain documentation to support all claims. The FTO's documentation should contain, but is not limited to the following:

- a. An initial notation of what phase, week numbers, and dates the FTO worked with the recruit.
- b. The total number of days the FTO worked with the recruit.
- c. A description of incidents the recruit was exposed to, accomplishments and difficulties encountered, and any remediation initiated. This documentation should be supported by dates, times, locations, and service numbers, where appropriate.
- d. An assessment of the recruit's potential as a police officer,

- e. A specific recommendation for retention or dismissal as an employee, generally, only the primary and any Intensive Remediation FTO's should make this recommendation. Any Relief FTO's that make this recommendation should do so at the discretion of the FTO Supervisor.
2. The FTO Supervisor's Cover Memorandum: This memo should briefly summarize the FTO's memo and contain a specific recommendation for retention or dismissal as an employee. This document should also contain:
    - a. An overall assessment of the recruit's performance to date,
    - b. The recruit's ability or lack of ability, to benefit from further remediation.
    - c. The recruit's overall potential to perform the duties of a Peace Officer.
  3. The Recruit Officer's Police Recruit Guide: This should be printed and presented at the termination meeting.
  4. A Copy of All FTO Related Reports: A copy of each should be found for review:
    - a. All D.O.R.'S
    - b. All Weekly Supervisor Reports
    - c. All End-of-Phase Reports
  5. Associated Administrative Letters and Memorandums: An original of each of the following should be included in this package:
    - a. A memo addressed to the Chief of Police, noting a review by the FTO Supervisor, of relevant documents (See Example 7-1).
    - b. A memo addressed to the Chief of Police, recommending the status of rehire for the Recruit (See Example 7-2).

As the Termination Package goes up through the chain of command, each officer in the chain shall note his concurrence on the sergeant's memo or

attach a memo explaining non-concurrence.



**CITY OF TEAGUE**

**OFFICE MEMO**

TO: DeWayne Philpott, Chief of Police

FROM: \_\_\_\_\_, FTO Supervisor

SUBJECT: **Termination: Recruit Police Officer**\_\_\_\_\_

DATE:

I have reviewed the letter to Officer \_\_\_\_\_ advising of his termination. It is in the correct form.

\_\_\_\_\_

FTO Supervisor

**CITY OF TEAGUE**

**OFFICE MEMO**

TO: DeWayne Philpott, Chief of Police

FROM: \_\_\_\_\_, FTO Supervisor

SUBJECT: **Recommendation for Rehire of** \_\_\_\_\_.

**DATE:**

Officer \_\_\_\_\_ was terminated from this Department on \_\_\_\_\_, 20\_\_\_\_, for his inability to follow instructions and the use of excessive force. Because of his prior record, I recommend that he not be rehired as a member of the Teague Police Department.

\_\_\_\_\_

FTO Supervisor

## ***TERMINATION***

The Chief of Police will make the final decision to recommend termination of the recruit to the Board of Aldermen. Once he has reached this decision, the chain of command will be notified, and the recruit will be scheduled to report to the FTO Supervisor's Office.

The FTO Supervisor will advise the recruit of the Chief of Police's decision and of the Department's intent to discharge him. As a matter of policy, a recruit may discuss the termination recommendation with anyone in the chain of command up to the level of FTO Supervisor. If the recruit expresses a desire to do so, the appropriate appointments will be made. Should the recruit choose to resign after the decision to terminate has been made, the Termination Package will be completed and maintained for future reference.

A recruit's training file is confidential and shall be reviewed only by persons connected with the Program or by persons having a "need to know." Others desiring a review of any file shall first secure approval from the Chief of Police. Agencies conducting background checks on former employees will be directed to the Chief for information. Access to a recruit's training file will be granted only in accordance with the Department's guidelines for release of confidential information or statutory law.

# TEAGUE POLICE DEPARTMENT

## FIELD TRAINING MANUAL



POLICE OFFICER TRAINEE

---

NAME

## RECRUIT TRAINING GUIDE

Organizational Procedures	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Duty hours and roll call procedures</b>		
<b>B. TCOLE 1999 Training</b>		
<b>1. Civil Service</b>		
<b>2. Compensation; including overtime and vacation time</b>		
<b>3. Personnel files and other employee records</b>		
<b>4. Management-employee relations in law enforcement organizations</b>		
<b>5. Work-related injuries</b>		
<b>6. Complaints and investigations of employee misconduct</b>		
<b>7. Disciplinary actions and the agency's internal appeal process</b>		
<b>C. Requirements to keep the department advised of current address and telephone number (Policies)</b>		
<b>D. Leave (City and Departmental Policy)</b>		
<b>1. Vacation</b>		
<b>2. Holidays</b>		
<b>3. Sick Leave</b>		
<b>4. Injured; on duty and off duty</b>		
<b>5. Death in the family</b>		
<b>6. Military Leave</b>		
<b>7. Leave without Pay</b>		
<b>8. Suspension</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

## RECRUIT TRAINING GUIDE

Holding Facility Procedure	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Booking Paperwork</b>		
<b>1. Completion of Freestone County Booking Sheet</b>		
<b>2. Inventory of Prisoner Property &amp; Signature on Booking Sheet</b>		
<b>3. Release of Prisoner Property at Scene – Only with their consent (Document Whom it was released to)</b>		
<b>B. Magistrate of prisoner (Municipal Court)</b>		
<b>1. Disposition of fines</b>		
<b>2. Types of payments accepted (Accepted at Police Department); After 5:00PM - Take to Jail</b>		
<b>3. During Normal working hours subjects taken to municipal court if Judge is available, otherwise take to jail.</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_

Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_

Date

## RECRUIT TRAINING GUIDE

Organizational Procedures Use of Force	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Use of force Continuum (Chapter 6 Department Policy)</b>		
<b>B. Use of Force (Chapter 6 Department Policy and Chapter 9 Penal Code)</b>		
<b>C. Deadly force (Chapter 6 Department Policy and Chapter 9 Penal Code)</b>		
<b>D. Duty to Intervein and Report (Chapter 6 Department Policy)</b>		
<b>I. Weapons (6.1 &amp; 6.2 Departmental Policy)</b>		
<b>1. Duty Pistol (Departmental Qualification)</b>		
<b>2. Patrol Shotgun (Departmental Qualification)</b>		
<b>3. Patrol Rifle (Departmental Qualification)</b>		
<b>4. Taser ECD (Certificate on Hand)</b>		
<b>5. PR- 24 (Certificate on Hand)</b>		
<b>6. OC Spray (Certificate on Hand)</b>		
<b>7. Centurion Control Stick (Certificate on Hand)</b>		
<b>8. ASP Baton (Certificate on Hand)</b>		
<b>9. Open hand Techniques</b>		
<b>10. Handcuff Techniques</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_

Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_

Date

## RECRUIT TRAINING GUIDE

Preparation for Patrol	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Personal Appearance and Hygiene (4.4 Departmental Policy)</b>		
1. Uniform / Cleanliness		
2. Haircuts and Facial Hair		
3. Shined/Serviceable Boots		
4. Tattoo Policy		
<b>B. Procedure in checking out supplies and equipment</b>		
1. Ticket / Warning Books		
<b>C. Learning of Geographical layout of City</b>		
1. Streets and business locations		
2. Assigned zones and areas of responsibility		
3. Security and Business Checks		
<b>D. Maintenance of Vehicles (9.03 City, 7.14 Department Policy)</b>		
1. Fueling procedure		
2. Checking of vehicle fluids prior to shift		
3. Completion of Vehicle Inspection/Repair Form		
<b>E. Searching vehicle prior to starting of shift</b>		
1. Check entire vehicle for contraband		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date



## RECRUIT TRAINING GUIDE

Preparation for Patrol	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>F. Procedures in getting vehicles repaired (7.14 Department Policy)</b>		
<b>1. Vehicle Inspection/Repair Form Submission</b>		
<b>G. Proper operation of Police Radio (Patrol SOP)</b>		
<b>1. Channels/Zones/Etc.</b>		
<b>2. Voice, Volume of speech, position of Microphone</b>		
<b>3. Use of Phonetic Alphabet</b>		
<b>4. Proper Radio Etiquette</b>		
<b>5. Use of 10 codes</b>		
<b>H. Policy regarding use of Emergency Equipment (7.14 Departmental Policy)</b>		
<b>1. Traffic Stops</b>		
<b>2. Code 3 (Properly notify Dispatcher)</b>		
<b>3. Pursuit Policy</b>		
<b>4. Completion of Pursuit form</b>		
<b>I. Stolen Vehicle Procedure</b>		
<b>1. Enter vehicle in TCIC/NCIC (Entry Forms on Share Drive)</b>		
<b>2. Recovery of stolen vehicle Procedure</b>		
<b>3. Processing of stolen vehicle Procedure</b>		
<b>4. Impounding &amp; Inventory Procedure</b>		
<b>5. Printing of stolen vehicle Procedure</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date



## RECRUIT TRAINING GUIDE

Procedures in Operation of Patrol Vehicle / Traffic Violator Contact	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Proper Driving Techniques (7.14 Departmental Policy)</b>		
1. Setting a good example for the public		
2. Driving defensively		
3. Driving in inclement weather		
4. Abiding by traffic laws		
5. Familiar with laws governing Emergency vehicle operation		
<b>B. Traffic Violators (7.30 Departmental Policy)</b>		
1. Identification		
2. Apprehension		
3. Proper Positioning of vehicle during stop		
4. Advising Dispatcher of the proper 10-28		
5. Advising Dispatcher of the proper stop location		
6. Using the seven-step method of violator contact		
<b>C. Procedure in felony traffic stops (Patrol SOP)</b>		
1. Officer safety		
2. Select stop location		
3. Use two patrol vehicles / Primary and Cover Unit		
4. Use Contact cover method suspect removal		
5. Proper Distance and positioning of patrol unit		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Basic Reports and Report Writing	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Criminal Reports / CopSync (Kologik)</b>		
1. Calls for Service – Enter all information		
2. Proper entry in computer		
3. Using proper arrest titles		
4. Completion of case information, (Including Person’s Involved)		
5. Completion suspect information portal		
6. Completion of narrative, evidence/property, NIBRS		
7. Completion of Supplements; recovered property, found property etc.		
8. Completion of persons involved; including driver’s license number, social Security number, address etc.		
9. Miscellaneous Fields – alias, tattoos, email, etc.		
<b>B. Traffic Citations</b>		
1. Completion of all information required on citation		
2. Officer Notes on Completion		
3. When written complaint is needed		
4. When arrest is made rather than issuance of citation		
5. Where do you get authority to arrest for traffic		
6. Issuance of warnings (traffic) when making arrests or for an actual traffic warning.		
<b>C. Search</b>		
1. Review consent to search exception/requirements		
2. What is Probable cause		
3. What is Reasonable Suspicion		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Basic Reports and Report Writing	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>D. Use of Field Notes / Interviews (7.1 Departmental Policy)</b>		
<b>1. Maintain a Field notebook</b>		
<b>2. Transcribe notes to reports</b>		
<b>E. Interview Techniques</b>		
<b>1. Field Interviews/Interrogations</b>		
<b>3. The use of intelligence bulletins (CopSync)</b>		
<b>4. Obtaining Witness/Suspect Statements</b>		
<b>5. Obtaining Suspect descriptions</b>		
<b>6. Obtaining description of property taken/value</b>		
<b>7. Miranda Warning (When it is / is not required)</b>		
<b>F. Evidence</b>		
<b>1. Proper method of submitting evidence</b>		
<b>2. Proper method of storage</b>		
<b>3. Chain of custody</b>		
<b>4. Photograph evidence</b>		
<b>5. Submission of bloody clothing</b>		
<b>6. Disposition of Class C Evidence (Photo &amp; Destroy)</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Procedures in Operation of Patrol Vehicle/ Emergency Driving	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Answering Emergency Calls (Refer to Patrol SOP)</b>		
1. Policy on utilizing Emergency Equipment		
2. Notifying Dispatcher Prior to Running Code 3		
3. Utilize direct or indirect approach to the crime scene		
4. Proper method of approaching scene		
5. Turning off emergency equipment/lights, siren prior to arrival.		
6. Park in area best suited for traffic direction		
<b>B. Pursuits (Chapter 7.15 Departmental Policy)</b>		
1. Policy on Pursuit driving		
2. Legal aspects of pursuits		
3. Responsibilities of pursuing officer		
4. Responsibility of the supervisor		
<b>C. Fire Calls (Patrol SOP)</b>		
1. Assist in traffic control		
2. Position patrol vehicle to protect fire hose		
3. Be conscious about crowd control		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Basic Patrol Techniques	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Officer's Responsibilities (Policy and Patrol SOP)</b>		
<b>1. Area of Responsibilities / Zone assignments</b>		
<b>2. Assisting other Law Enforcement Officers</b>		
<b>3. Be aware of what occurs in your assigned zone</b>		
<b>4. Be aware, through Calls for Service review and briefings, of prior shift activity</b>		
<b>5. Be observant of your surroundings</b>		
<b>B. Patrol Tactics (Patrol SOP)</b>		
<b>1. Always utilize Officer safety</b>		
<b>2. Use Contact cover techniques while contacting the public</b>		
<b>3. Respond to calls tactically</b>		
<b>4. Use Two Officers while dealing with domestic Violence</b>		
<b>5. Use Two or more Officers while serving Felony Warrants</b>		
<b>6. Handcuff and then Search when dealing with suspects</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Basic Patrol Techniques	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>C. Patrol Procedures (Patrol SOP &amp; City Ordinance)</b>		
1. Open doors/buildings		
2. Burglary in Progress		
3. Robbery in Progress		
4. Disturbance in progress		
5. Weapons Calls		
6. Multiple suspect fight call		
7. Suspicious Person		
8. Suspicious Vehicle		
9. Suicidal Person		
10. Security & Business check procedure		
11. Familiarity with City ordinance violations		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ **Date**

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ **Date**



## RECRUIT TRAINING GUIDE

Basic Patrol Techniques	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>D. Public Contacts</b>		
1. Treat all citizens with respect and dignity		
2. Utilize Community Policing Philosophy		
3. Visit with the public / encourage feedback		
4. Identify, Isolate, and take corrective action for problems		
5. Be accessible to the citizens you serve		
<b>E. Dealing with emotionally disturbed person's</b>		
1. Peace Officer Emergency Order of Detention Form (Share Drive) and procedures		
2. Responsibility to the EDP		
3. Justice of the Peace Emergency Order of Detention Procedures		
<b>F. Dealing with transients, etc.;</b>		
<b>G. Procedure in dealing with public gatherings (Chapter 8.0 &amp; 8.1 Departmental Policy)</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Basic Patrol Techniques	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>H. Assisting other agencies</b>		
1. Sheriff's Office		
2. Constable's Office		
3. Other Municipal Agencies		
<b>I. Specific Contacts</b>		
1. Death Notification (Patrol SOP)		
2. Solicitors, Peddlers and Salesman (Section 4.402 City Ordinance)		
<b>J. Civil Matters</b>		
1. Landlord complaints (Property Code)		
2. Evictions (Property Code)		
3. Repossessions		
4. Civil Standby's – not done except for FV cases, with supervisor approval, or court ordered.		
5. Property disputes /divorces		
6. Child Custody matters		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Basic Patrol Techniques	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>K. Public Service</b>		
1. Medical aid		
2. Stranded motorist		
3. General Information: directions etc;		
4. Walk in complaints		
5. Referring complaints		
6. Officer complaints (Procedures – Police 2.3 & 2.4)		
7. Security checks of homes / Businesses		
8. Dealing with the press, who's responsibility		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Basic Patrol Techniques	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>L. Handling Juveniles (7.12 Departmental Policy)</b>		
1. Taking juvenile into custody		
2. Searching of juveniles		
3. Obtaining statements from juveniles		
4. When to Magistrate Juveniles		
5. Questioning of juveniles		
6. Transporting of juveniles to the detention center		
7. Fingerprinting of juveniles		
8. Photographing of juveniles		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Accident Investigation (7.31 Departmental Policy)	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Accidents (Patrol SOP)</b>		
1. Minor accident		
2. Major accident		
3. Fatal accident		
4. Failure to meet requirements / vehicle, fixed object		
5. Failure to stop and render aid		
6. Accident private property		
7. Accident involving a motorcycle / bicycle		
8. Accident involving a pedestrian		
9. Accidents involving city equipment and personnel		
10. Reporting requirements/procedures (CRASH Report)		
<b>B. Handling of Injured Persons</b>		
1. Keep victim calm until ambulance arrives		
2. Ensure the scene is contained		
3. Prevent theft from occurring		
4. Ensure traffic safety vests are always utilized		
<b>C. Traffic direction</b>		
1. Ensure vehicles are positioned to protect victims		
2. Place cones / road flares when/where appropriate		
3. Ensure traffic safety vests are always utilized		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Accident Investigation	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>D. Proper and timely completion of forms</b>		
1. CRASH Report Process (online reporting)		
2. Be familiar with Clock positions/direction of impact		
3. Be familiar with damage rating scale		
4. Be familiar with determining traffic or criminal action		
<b>E. Following up on evidence at scene</b>		
1. Failure to meet requirements upon striking object or vehicle		
2. Failure to stop and render aid		
3. Following debris trail during accident		
4. Taking measurements and when are they required at an accident scene		
5. Complete a scale diagram when required		
6. Treat evidence collecting like any other criminal Investigation.		
7. Identify witnesses		
8. Take statements from victims and witnesses		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Arrest Procedures (7.2 & 7.7 Departmental Policy)	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. How to Arrest</b>		
1. Identify the offense		
2. Decide to apprehend		
3. Apprehend		
<b>B. Types of Arrest</b>		
1. Arrests of subjects in vehicle		
2. Arrests of subject in a public place		
3. Arrests of subject from homes		
4. Guarding suspects in custody at medical facilities		
5. Use of restraints on suspects		
6. Where do you get the authority to arrest without warrant		
<b>C. Transporting Prisoners</b>		
1. In police vehicle		
2. Transporting opposite sex – Give Mileage		
3. Transporting of all Juveniles – Give Mileage		
4. Search Vehicle before/after arrested person is in vehicle.		
5. Ensure that prisoners are searched and secured properly prior to transport		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Family Violence Contacts	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Dealing with Family Violence</b>		
1. Respond in a timely manner		
2. Approach with Caution		
3. Separate subjects and interview		
4. Determine if an offense has occurred		
5. Identify victim or victims		
6. Provide medical treatment if needed		
7. Take action regarding the offense that has occurred		
8. Obtain photographs		
9. Obtain statements from victim and witnesses		
10. Provide victims assistance		
11. Ensure victims receive rights/compensation package		
12. Complete appropriate paperwork ie; Emergency Protective order		
13. Knowledge of Emergency protective order process		
14. Knowledge of permanent protective order process		
15. Knowledge of available victim Services ie; counseling		
16. Process in providing battered spouse shelter/location		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date



## RECRUIT TRAINING GUIDE

Traffic Enforcement Procedures and Operation of Special Equipment	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Specific Enforcement</b>		
1. Use of Radar (S.O.P.)		
2. Certification of Radar		
3. Moving Radar		
4. Stationary Radar		
5. Parking violations		
6. Handicap parking violations		
7. Pedestrian violations		
8. School zone enforcement		
<b>B. Procedure in identifying driver</b>		
1. Driver's License number or name and date of birth		
<b>C. Procedure in identifying vehicles</b>		
1. Registration by plate number or VIN number		
<b>D. Procedure in dealing with out of state violators (Non-Resident Violator Compact)</b>		
<b>E. Municipal Court procedures</b>		
1. Appearances		
2. Court dates		
3. Court room demeanor		
4. Court room security		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Complaints and Affidavit Procedure	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Complaint</b>		
1. When is complaint needed		
2. How to complete complaint		
<b>B. Affidavit</b>		
1. When is affidavit needed		
2. How to complete affidavit		
<b>C. Method in submitting complaint and affidavit for warrant</b>		
<b>D. Where to submit the warrant &amp; receipt for the warrant</b>		
<b>E. Procedure after warrant is issued</b>		
<b>F. Types of Warrants</b>		
1. What is difference between a Capias warrant and other warrants		
2. What is a Capias Pro Fine?		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_

**Date**

FTO Signature: \_\_\_\_\_

\_\_\_\_\_

**Date**

## RECRUIT TRAINING GUIDE

Handling Evidence and Recovered Property (Policy 12.0 and Texas DPS Crime Lab Submission Manual)	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Recovered Property</b>		
1. Bicycles		
2. Money, wallets, and jewelry		
3. Any other valuable items		
<b>B. Use of Evidence lockers</b>		
1. Method of storage		
2. Items too large for evidence lockers		
3. Properly marking of evidence		
4. Utilization of proper evidence tags		
5. Proper marking of Weapons		
6. The method of collecting and processing Class C evidence		
7. The proper method of DPS lab submission (Lab Submission Manual – TXDPS)		
<b>C. Obtaining evidence for court</b>		
1. How to obtain evidence		
2. Who to contact regarding evidence		
3. What to do with returned evidence		
4. Importance of custody control while in possession of evidence.		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Court Appearance and Legal Process	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Court Appearances (Police 2.6)</b>		
1. Municipal Court		
2. County /District Court		
3. Grand Jury		
4. Civil Court		
<b>B. Court Room Procedures</b>		
1. Court Room Demeanor		
2. Invoking the Rule		
3. Talking to the Jury		
4. Talking to the Prosecuting Attorney		
5. Talking to the defendant		
<b>C. Legal Processes</b>		
1. Search Warrant (CCP) (Policy 7.2, 7.3, & 7.4)		
2. Arrest Warrants (CCP) (Policy 7.2, 7.3, & 7.4)		
3. Receiving Summons, Subpoenas		
4. County/District Standby Procedures		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_

Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_

Date

## RECRUIT TRAINING GUIDE

Disciplinary Procedures	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Officer Complaints (Policy 2.3)</b>		
1. Requirements for making Formal Complaints		
2. Anonymous Complaints		
3. Confidentiality		
4. Officers Written Statements		
<b>B. Internal Investigations (Policy 2.3)</b>		
1. Officers Rights		
2. Requirements to answer questions		
3. Garrity Warning		
4. Supervisors Presence during Interview		
5. Counsel presence during Interview		
6. Miranda Warning		
7. Search of Department owned Equipment		
8. Special Examinations		
9. Appeal Process		
<b>C. Grievance Procedures (Policy 4.6 &amp; City Policy 13.07)</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Evaluation Procedures and Racial Profiling	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Officer Evaluations (Policy 4.3 &amp; Evaluation Manual)</b>		
1. Requirements for Evaluations		
2. Method of Evaluation		
3. Importance of Documentation		
4. Goals for Officers		
5. Reviewing of Evaluations		
<b>B. Racial Profiling (Policy 2.1)</b>		
1. What is Racial Profiling		
2. How does Racial Profiling affect the Officer/Department		
3. Departments position on Racial profiling		
4. Officers responsibility on reporting Racial Profiling Violations in the Department		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_

**Date**

FTO Signature: \_\_\_\_\_

\_\_\_\_\_

**Date**

## RECRUIT TRAINING GUIDE

Off Duty Enforcement / Off Duty Employment	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Off Duty Enforcement</b>		
1. How to handle Misdemeanor violations		
2. Felonies committed in your presence		
3. Understanding Jurisdictional boundaries		
4. Utilization of Good Judgment		
5. No stopping of violators in your personally owned vehicle		
<b>B. Off Duty Employment (Policy 4.5)</b>		
1. Procedure in requesting an off-duty job		
2. Procedure in working Security		
3. The method of compensation		
4. Duties in reporting off duty injuries		
5. Demeanor during off duty jobs		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_

Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_

Date

## RECRUIT TRAINING GUIDE

Responding to Alarms	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Residential Alarms (Patrol SOP)</b>		
1. Respond quietly and safely to the scene		
2. Position vehicle at a minimum of 2 houses from alarm		
3. Tactically approach using cover and concealment		
4. Stop prior to reaching residence and listen and evaluate		
5. Ensure you have sufficient officers for the alarm call		
6. Use Contact Cover technique to search residence		
7. Never pull up in front residence		
8. Never search residence alone		
<b>B. Business Alarms (Patrol SOP)</b>		
1. Respond quietly and safely to the scene		
2. Position vehicle at a minimum of 1 building from alarm		
3. Tactically approach using cover and concealment		
4. Stop prior to reaching business and listen and evaluate		
5. Ensure you have sufficient officers for the alarm call		
6. Use Contact Cover technique to search business		
7. Never pull up in front of business		
8. Never search business alone		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date



## RECRUIT TRAINING GUIDE

CID call out / Hostage Situations	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Supervisor/Officer Call Out</b>		
1. Proper procedure for calling Supervisors to a crime scene		
2. When do you call out a Supervisor to a crime scene		
3. What is the patrol officer's responsibility when assisting Supervisors at a crime scene		
4. What precautions do you need to take at a crime scene (Policy 7.41)		
5. Supervisors call additional officers, unless they are unavailable or an emergency exists.		
<b>B. Hostage situations and Swat Team (Patrol SOP)</b>		
1. What is the Policy for handling Hostage situations		
2. What are the procedures in notifying appropriate personnel		
3. What is the patrol officers responsibility at the scene		
4. What is the Hostage Negotiators function		
5. What is the Swat teams function		
6. Who is in charge at the scene		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Basic Patrol Functions	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Missing Persons Procedures (Patrol SOP)</b>		
1. Missing Child		
2. Missing Adult		
3. Runaway		
4. Welfare concern		
<b>B. Animal Complaints (City Ordinance and Texas Statutes)</b>		
1. Cruelty to Animals		
2. Animal Control Officers		
3. Found Animals		
4. Dead Animals		
5. Shooting of Animals by Officers		
6. Dog Complaints		
7. Prisoner's Animal		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_

Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_

Date

## RECRUIT TRAINING GUIDE

Penal Code	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Chapter 2</b>		
1. Reasonable doubt		
2. Affirmative defense		
<b>B. Chapter 6</b>		
1. Culpability		
2. Culpable States		
<b>C. Chapter 7</b>		
1. Parties to offense		
2. Criminal Responsibility		
<b>D. Chapter 8</b>		
1. Defenses of Responsibility		
<b>E. Chapter 9</b>		
1. Deadly force		
2. Self Defense		
3. Arrest and Search		
<b>F. Chapter 12</b>		
1. Misdemeanor Punishment		
2. Felony Punishment		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_

Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_

Date

## RECRUIT TRAINING GUIDE

Penal Code	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>G. Chapter 19</b>		
1. Murder		
2. Capital Murder		
3. Manslaughter		
4. Criminal Negligent Homicide		
<b>H. Chapter 20</b>		
1. Kidnapping		
<b>I. Chapter 21</b>		
1. Sexual Offenses		
2. Indecency with a child		
<b>J. Chapter 22</b>		
1. Assaultive offenses		
2. Injury to a child		
3. Deadly Conduct		
4. Terroristic Threat		
<b>K. Chapter 25</b>		
1. Offenses against the Family		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Penal Code	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>L. Chapter 28</b>		
1. Arson		
2. Criminal Mischief		
3. Reckless Damage or Destruction		
<b>M. Chapter 29</b>		
1. Robbery		
2. Aggravated Robbery		
<b>N. Chapter 30</b>		
1. Burglary		
2. Burglary of Vehicles		
3. Criminal Trespass		
<b>O. Chapter 31</b>		
1. Theft		
<b>P. Chapter 32</b>		
1. Fraud		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Penal Code	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>Q. Chapter 36</b>		
<b>1. Obstruction or Retaliation</b>		
<b>R. Chapter 37</b>		
<b>1. Perjury</b>		
<b>2. Tampering with Governmental Record</b>		
<b>S. Chapter 38</b>		
<b>1. Failure to Identify</b>		
<b>2. Resisting Arrest, Search and Evading Arrest or Detention</b>		
<b>3. Hindering Apprehension</b>		
<b>T. Chapter 39</b>		
<b>1. Abuse of office</b>		
<b>2. Official Oppression</b>		
<b>U. Chapter 42</b>		
<b>1. Disorderly Conduct and Related Offenses</b>		
<b>2. Harassment</b>		
<b>3. Stalking</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Penal Code	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>V. Chapter 43</b>		
<b>1. Public Indecency</b>		
<b>W. Chapter 46</b>		
<b>1. Unlawful Carrying weapons</b>		
<b>2. Unlawful possession of a firearm</b>		
<b>3. Making a firearm accessible to a child</b>		
<b>X. Chapter 47</b>		
<b>1. Gambling</b>		
<b>Y. Chapter 49</b>		
<b>1. Public Intoxication</b>		
<b>2. Driving While Intoxicated - No citations for traffic offense</b>		
<b>Z. Chapter 71</b>		
<b>1. Organized Crime</b>		
<b>2. Engaging in Organized Criminal Activity</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

## RECRUIT TRAINING GUIDE

Code of Criminal Procedure	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Chapter 15</b>		
1. Warrant of Arrest	Art. 15.01	
2. Complaint	Art. 15.04	
<b>B. Chapter 17</b>		
1. Personal Bond	Art. 17.03	
2. Release on Personal bond	Art. 17.031	
3. Magistrates order for emergency protection	Art. 17.292	
<b>C. Chapter 18</b>		
1. Search warrants	Art. 18.01	
<b>D. Chapter 23</b>		
1. Capias	Art. 23.01	
2. Capias or summons in felony	Art. 23.03	
<b>E. Chapter 24</b>		
1. Subpoena	Art. 24.01	
2. Subpoena duces tecum	Art. 24.02	

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date



## RECRUIT TRAINING GUIDE

Sexual Harassment in the Workplace (Policy 2.2 & City Policy 12.04)	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>A. Sexual Harassment</b>		
<b>1. What is Sexual Harassment?</b>		
<b>2. Complaint Procedure</b>		
<b>3. What is the City Policy</b>		
<b>4. What is the Department Policy</b>		
<b>5. How does it affect the individual</b>		
<b>6. How does it affect the working environment</b>		
<b>7. What steps can be taken to avoid Sexual Harassment</b>		
<b>8. Who is subject to Sexual Harassment</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_

Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_

Date

## RECRUIT TRAINING GUIDE

Transportation Code	Instructional Method	Actual Field Experience
	Date / FTO	Date / FTO
<b>Knowledge of the Transportation Code</b>		
<b>1. Movement of vehicles on Roadway</b>		
<b>2. Registration of Vehicles</b>		
<b>3. License Requirements</b>		
<b>4. Suspension of License</b>		
<b>5. DWLI</b>		
<b>6. Implied consent law</b>		
<b>7. Speeding Restrictions</b>		
<b>8. Reckless Driving Offense</b>		
<b>9. Accident Reports</b>		
<b>10. Financial Responsibility Requirements</b>		
<b>11. Miscellaneous Laws</b>		
<b>12. Open Container Vehicle P.C 49.031</b>		

The Above Subjects were explained to me and I have performed them and / or have been tested to determine my knowledge of them.

Recruit Officers Signature: \_\_\_\_\_

\_\_\_\_\_ Date

FTO Signature: \_\_\_\_\_

\_\_\_\_\_ Date

**TEXAS COMMISSION ON LAW ENFORCEMENT  
OFFICERS STANDARDS AND EDUCATION  
6330 U.S. Highway 290 East, Suite 200  
Austin, Texas 78723  
(512) 936-7700**

**SEVEN STEP APPROACH**

Most of the public contacts made by police are made around traffic stops. While officers must be aware of the total traffic situation and be able to intelligently relate this problem to the driving acts of the public, we must also realize that a great number of violators have never been Stopped, and many do not realize why they are being stopped.

Good officer- violator relations not only promote good public relations, but also make the job of an officer easier. The following procedure should be considered as a guideline that will enable each officer to develop self – confidence in violator relationships through knowledge.

1. **Greeting and Identification of the Police Agency**

The greeting may be accomplished in the most natural way for the officer. He / She may introduce himself / herself, or use only a “Good Morning,” “How do you do Sir?” or other natural greeting. This is a courtesy we owe to every citizen stopped. Regardless of whether the officer is in a marked car and in uniform, he / she should identify himself / herself and name his/her agency. The objectives in greeting are to employ business courtesy, to help make the subject feel at ease, and to establish a common ground free of affection, superiority, or deference. Smile and Speak in a quiet voice. Remember there are many citizens, and a great number may not reside on your locale and therefore do not recognize your uniform. Put yourself in their position and you can readily see why a greeting and identification of the agency you represent are important, not only to the violator, but to the success of your contact.

2. **Statement of Violation Committed**

The officer owes the driver the courtesy of telling him/her at once the reason he / she has been stopped. This step should emphasize the seriousness of the violation and serve to create a proper effect upon the violator. If the case is one of speeding, the officer should ascertain whether attending circumstances might morally justify such speed to a normal, prudent person. After he/she is told of the violation for which he/she has been stopped, the question, “Is there any reason for your excessive rate of speed?” offers the subject an opportunity to justify his / her actions if a reason exists, and if none, places him / her in a position of admitting the violation. However, with the above exception, one should refrain from asking questions concerning the subject’s knowledge of the violation committed. Remarks made by the officer should be in a form of a statement rather than a question.

3. **Identification of Driver and Check of Conditions of Violator &Vehicle**

The officer should identify every violator stopped by requesting his operators’ license. The officer should ask for other forms of identification, preferably something which has the person’s description and photograph, if they have no license or identification card. If the subject has none, the officer should write down a brief description of the person: age, height, weight, eyes, hair, marks, and address.

The officer, after identifying the subject, should call him or her by name during the remainder of the interview. Should a violator hand an operator's license to you in a purse or billfold, have him / her remove the license themselves so that no accusation can be made about loss of money or important papers. A close comparison should be made between the the description of the individual and the description of the subject on the drivers license.

4. Statement of Action to be taken

**The officer should make a clear statement, in a firm but calm manner, that will leave no**

**Doubt to the actions he/she plans** Example: "you will be charged with the offense of speeding in the Municipal Court for Teague, Texas. You will be given 10 days (Specify procedure) in which to answer the charge. You are going to be charged with the offense of passing with insufficient clearance. You will be warned this time for the degree of violation which you have committed. A record of this violation has been made and we ask that you cooperate by driving your vehicle in compliance with traffic regulations." Patrolman should practice the technique of refraining from the use of "I" during the violator interview. Place the emphasis on the violator, and the violation committed to be taken by the officer and affords the violator an opportunity to shift the blame from the offense committed to the action taken by the officer. When the "you" technique is practiced, much unpleasantness is avoided.

5. Take that Action

Write the citation, take the violator into custody, or call his / her attention to the seriousness of the violation and possible consequences (Warning), and the action will have been taken in the manner the officer has decided.

6. Explain What the Violator Must Do

Explain to the violator exactly what action he / she must take, which is; He/ she must appear at a certain court by a certain date / time and before a certain Magistrate, or refrain from repeating a certain violation. A short explanation serves to dispel much uncertainty in the mind of the violator. Make your explanation clear and be sure the violator understands. Remember, he/she is not as familiar with the courts and the locations involved as you are. A little extra time here may result in more appearances on time and less warrants issued.

7. Leave

Closing the contact with the violator is awkward for many officers. It is an opportunity to create a feeling of friendliness if the proper technique is used. An attitude of officiousness or gloating must be avoided. An expression of real friendliness by the officer and an attitude of helpfulness a service is desired. Do not overdo it, however; never give the subject any reason to think that you are sorry for having given him / her a ticket and that you now wish to "Oil the water." The leave-taking should be as firm and impersonal as the approach. A "Good Afternoon" or "Have a safe day" spoken in sincere, yet business-like tone, is sufficient. When the violator contact has been broken, do not hesitate, but immediately return to the patrol car and ensure that the violator has safely reentered traffic before proceeding on.

**Certification and Acknowledgement**

**I, \_\_\_\_\_, have received instruction from the FTO Staff as to my responsibilities as defined by the Teague Police Department Policy and Procedure Manual. They have also reviewed the Field Training Manual with me, and I understand that I must successfully complete the Field Training program to remain employed with the City of Teague.**

\_\_\_\_\_  
**Recruit Officer Signature**

\_\_\_\_\_  
**Date**

\_\_\_\_\_  
**Field Training Officer**

\_\_\_\_\_  
**Date**

\_\_\_\_\_  
**Patrol Sergeant**

\_\_\_\_\_  
**Date**

\_\_\_\_\_  
**Chief of Police**

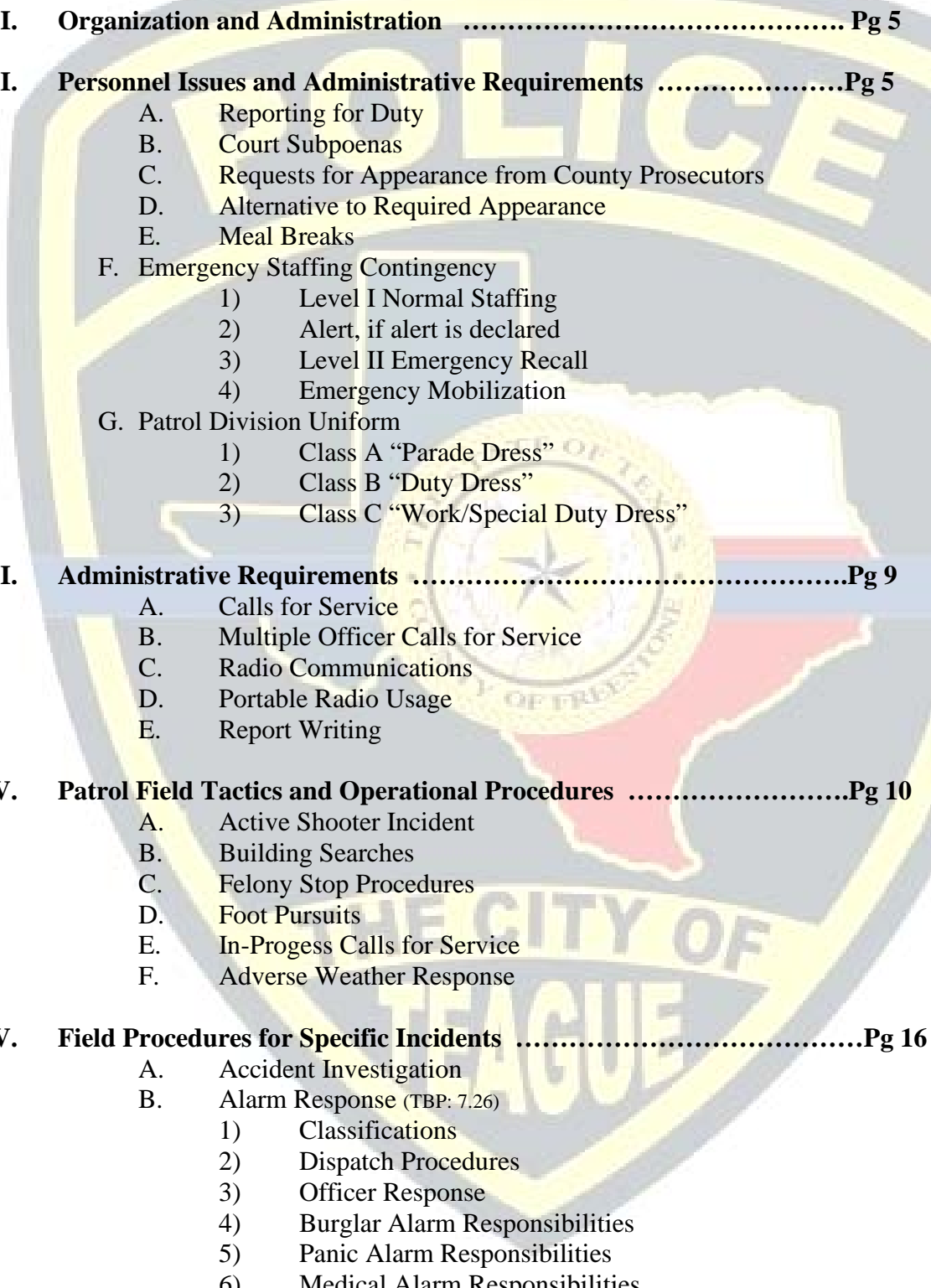
\_\_\_\_\_  
**Date**

# Teague Police Department



**Patrol**  
Standard Operational Procedures

# Table of Contents



**I. Organization and Administration ..... Pg 5**

**II. Personnel Issues and Administrative Requirements .....Pg 5**

- A. Reporting for Duty
- B. Court Subpoenas
- C. Requests for Appearance from County Prosecutors
- D. Alternative to Required Appearance
- E. Meal Breaks
- F. Emergency Staffing Contingency
  - 1) Level I Normal Staffing
  - 2) Alert, if alert is declared
  - 3) Level II Emergency Recall
  - 4) Emergency Mobilization
- G. Patrol Division Uniform
  - 1) Class A “Parade Dress”
  - 2) Class B “Duty Dress”
  - 3) Class C “Work/Special Duty Dress”

**III. Administrative Requirements .....Pg 9**

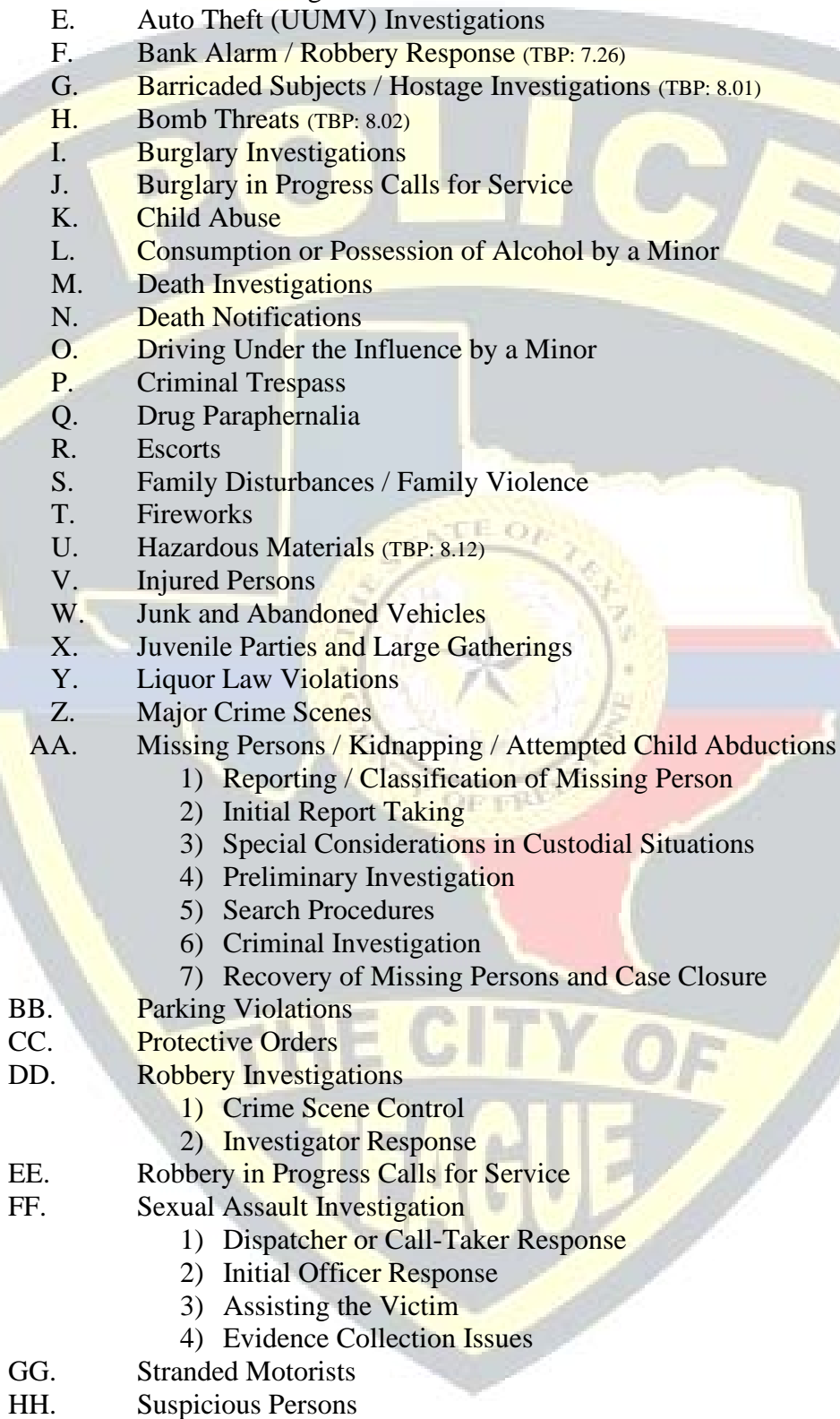
- A. Calls for Service
- B. Multiple Officer Calls for Service
- C. Radio Communications
- D. Portable Radio Usage
- E. Report Writing

**IV. Patrol Field Tactics and Operational Procedures .....Pg 10**

- A. Active Shooter Incident
- B. Building Searches
- C. Felony Stop Procedures
- D. Foot Pursuits
- E. In-Progress Calls for Service
- F. Adverse Weather Response

**V. Field Procedures for Specific Incidents .....Pg 16**

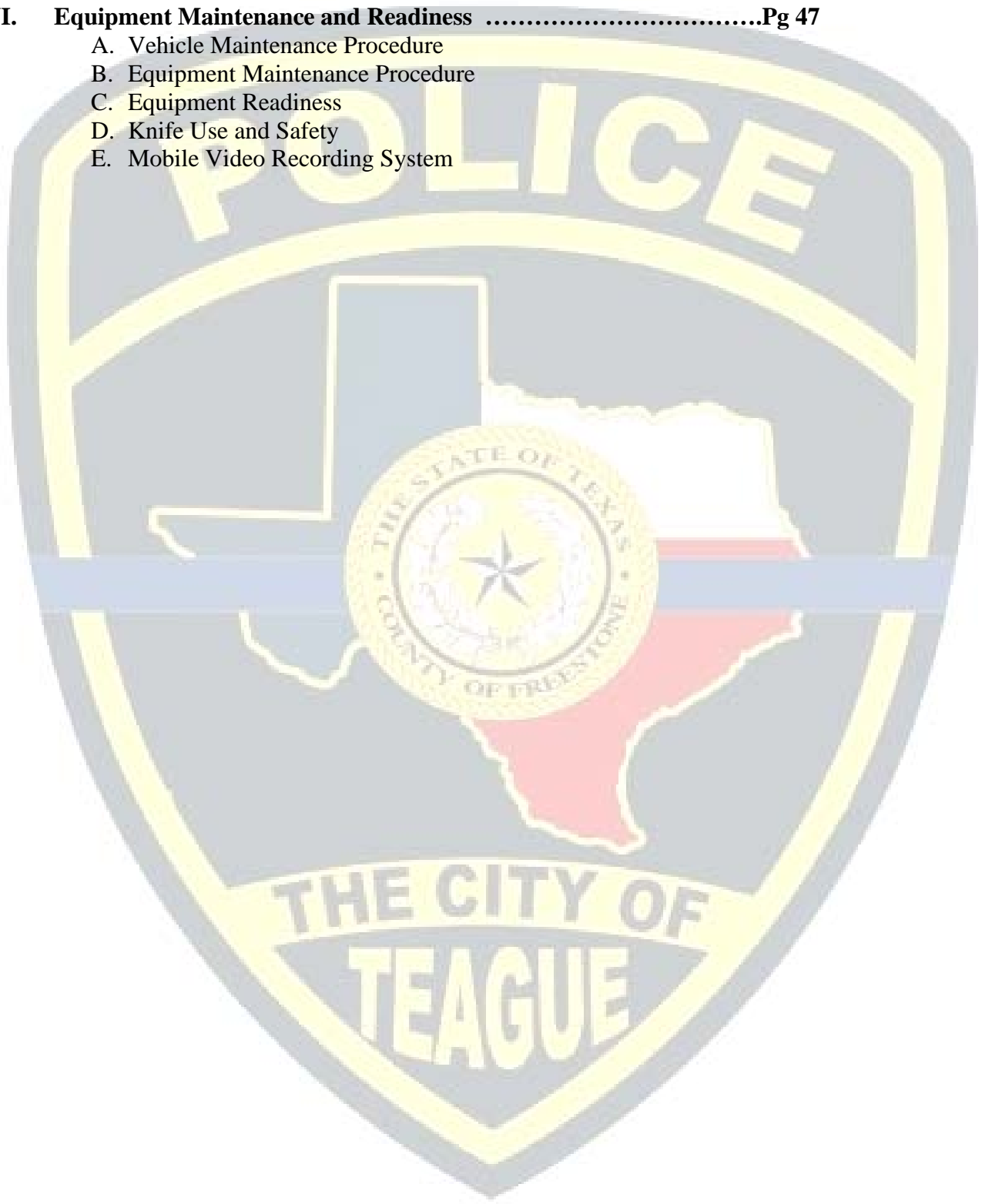
- A. Accident Investigation
- B. Alarm Response (TBP: 7.26)
  - 1) Classifications
  - 2) Dispatch Procedures
  - 3) Officer Response
  - 4) Burglar Alarm Responsibilities
  - 5) Panic Alarm Responsibilities
  - 6) Medical Alarm Responsibilities
  - 7) Fire Alarm Responsibilities

- 
- C. Arson Investigations
  - D. Assault Investigations
  - E. Auto Theft (UUMV) Investigations
  - F. Bank Alarm / Robbery Response (TBP: 7.26)
  - G. Barricaded Subjects / Hostage Investigations (TBP: 8.01)
  - H. Bomb Threats (TBP: 8.02)
  - I. Burglary Investigations
  - J. Burglary in Progress Calls for Service
  - K. Child Abuse
  - L. Consumption or Possession of Alcohol by a Minor
  - M. Death Investigations
  - N. Death Notifications
  - O. Driving Under the Influence by a Minor
  - P. Criminal Trespass
  - Q. Drug Paraphernalia
  - R. Escorts
  - S. Family Disturbances / Family Violence
  - T. Fireworks
  - U. Hazardous Materials (TBP: 8.12)
  - V. Injured Persons
  - W. Junk and Abandoned Vehicles
  - X. Juvenile Parties and Large Gatherings
  - Y. Liquor Law Violations
  - Z. Major Crime Scenes
  - AA. Missing Persons / Kidnapping / Attempted Child Abductions
    - 1) Reporting / Classification of Missing Person
    - 2) Initial Report Taking
    - 3) Special Considerations in Custodial Situations
    - 4) Preliminary Investigation
    - 5) Search Procedures
    - 6) Criminal Investigation
    - 7) Recovery of Missing Persons and Case Closure
  - BB. Parking Violations
  - CC. Protective Orders
  - DD. Robbery Investigations
    - 1) Crime Scene Control
    - 2) Investigator Response
  - EE. Robbery in Progress Calls for Service
  - FF. Sexual Assault Investigation
    - 1) Dispatcher or Call-Taker Response
    - 2) Initial Officer Response
    - 3) Assisting the Victim
    - 4) Evidence Collection Issues
  - GG. Stranded Motorists
  - HH. Suspicious Persons
  - II. Terrorist Screening Center



**VI. Equipment Maintenance and Readiness .....Pg 47**

- A. Vehicle Maintenance Procedure
- B. Equipment Maintenance Procedure
- C. Equipment Readiness
- D. Knife Use and Safety
- E. Mobile Video Recording System



# PATROL STANDARD OPERATING PROCEDURES

## I. ORGANIZATION AND ADMINISTRATION

- A. The Patrol Division is commanded by the Chief of Police who shall have authority to command all assigned personnel directly or through subordinate supervisors. The Patrol Sergeant reports to the Chief of Police.
- B. This Patrol Standard Operating Procedure will be maintained and reviewed by the Chief of Police. Changes to this SOP will be made by memorandum or email and will remain in effect until incorporated into a newer version. The SOP will be review annually by the Chief of Police for compliance with current operations and compliance with Texas law.
- C. All changes made in this SOP must be approved in writing by the Chief of Police.

## II. PERSONNEL ISSUES AND ADMINISTRATIVE REQUIREMENTS

### A. Reporting for Duty

- 1. Personnel report to duty at the time and place as assigned and/or scheduled, fully prepared and capable of performing their assigned duties.
- 2. Personnel beginning a tour of duty make themselves available to undertake their assignments immediately at the start of their tour of duty.
- 3. Personnel beginning tour of duty review previous shifts' activities, computer messages, memos, information posted, and other similar information media in order that the member is fully informed of necessary and pertinent information.

### B. Court Subpoenas and Appearances

- 1. Municipal Court requests for appearances will normally be transmitted via interoffice email. Officers will consider these requests or dockets as subpoenas and will attend the requested court session unless otherwise approved by the Court. Any inability to meet the requested appearance should be communicated to the Municipal Court as soon as possible by the officer.
- 2. Any and all subpoenas or requests for appearances from County, District or United States District Courts or the Attorney assigned to these Courts will be forwarded immediately to the Chief of Police whether received by telephone, fax or subpoena service. The Chief of Police will forward the request or subpoena to the Patrol Sergeant and notify the officer. Any inability to respond appropriately to the request or subpoena will be communicated to the requesting attorney as soon as possible by the officer, after notifying the chain of command.

C. Requests for Appearance from County Prosecutors.

1. Officers who receive notice of a Request for Appearance from the Freestone County or District Attorney's Office will consider the request as a subpoena and as a required assignment by this department. Officers are to attend the court as requested at the time and place requested unless notified by the Prosecutor assigned to the case, the Clerk of the Court, or other departmental authority.
2. In case of a notice to disregard, the officer should note the date, time and name of the notifying individual for future reference as needed.

D. Alternative to Required Appearance.

1. Officers who, for various reasons, need to be on standby to attend court, unless their appearance is absolutely required, may attempt to utilize the following procedure;
  - a. Contact the prosecutor assigned to the case prior to the day of the request for appearance.
  - b. Ask permission of the prosecutor to be placed on "Stand-by" for the appearance.
  - c. Discuss the details of the case with the prosecutor at that time if possible.
  - d. Provide the prosecutor with your phone number, including alternate method of contact.
  - e. Officers who are allowed by the Prosecutor to be on "Stand-by" must be able to respond appropriately dressed within one hour. Failure to respond to a "Stand-by" call may result in the case being dismissed.
  - f. Officers who are on "Stand-by" are not compensated unless they are called to court and then only for the time in court plus travel time. Officers who are on stand-by will remain on stand-by until released earlier by the prosecutor or the secretary of the court. Officers should understand that some cases will require in person attendance and Stand-by will not be available.

E. Meal Breaks

1. No more than three uniformed officers and two marked police vehicles will meet and check out at any eating establishment. The exception to this is:
  - a. When uniformed officers are attending departmental functions. or
  - b. When approved by the immediate supervisor.
2. Length of Meal Breaks
  - a. In accordance with FLSA officers are compensated for their mealtime and are not guaranteed a meal break. If the officer has an opportunity to take a meal break it should be no longer than 60 minutes.

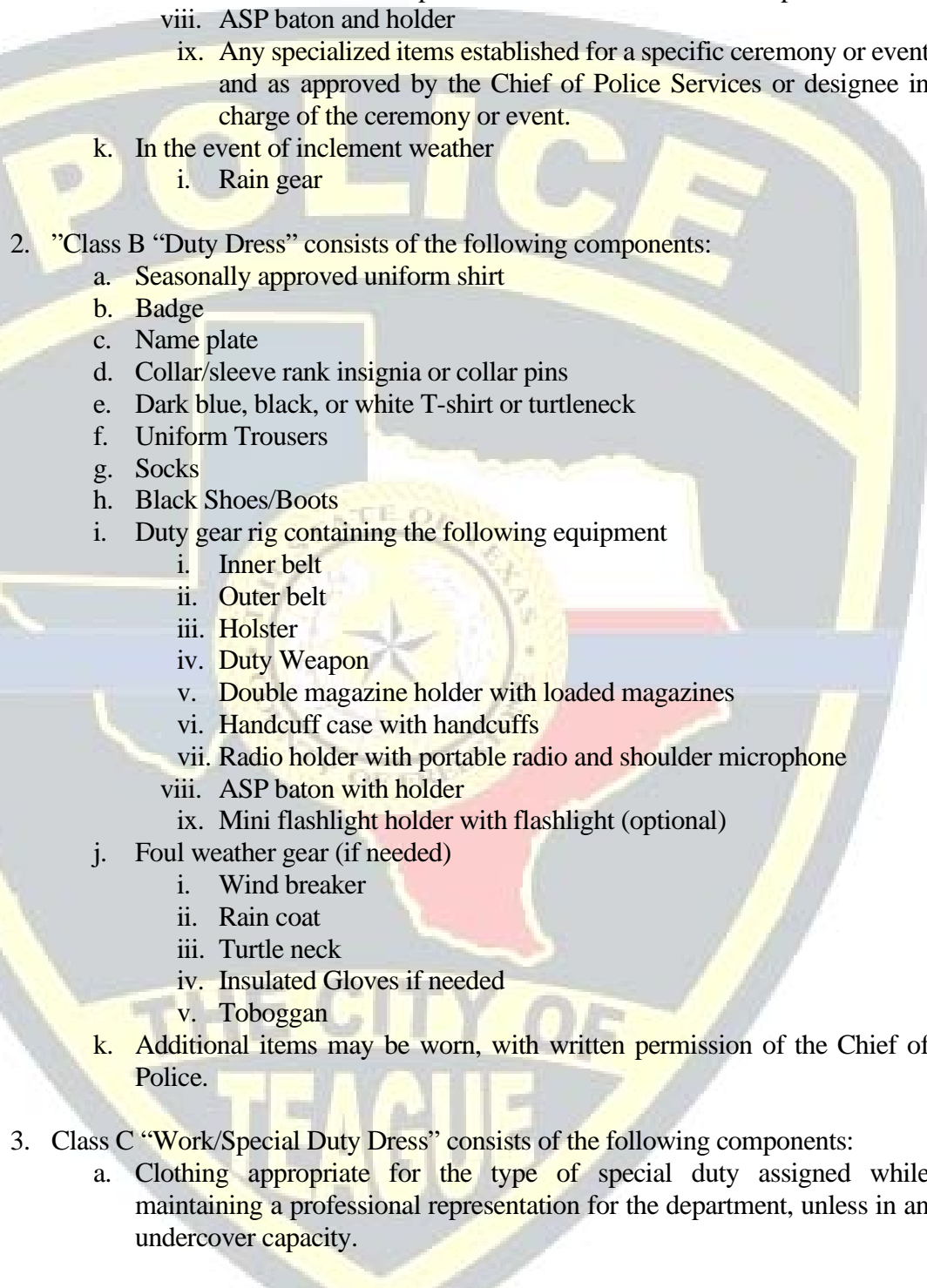
## F. Emergency Staffing Contingency

The following schedule is followed in the event of an emergency.

1. Level I Normal Staffing
  - a. Patrol On-Call available if needed
  - b. Normal readiness
  - c. All officers have phones available
  - d. 2-hour response capability if called for service
2. Alert: If an Alert is declared
  - a. All Officers will have a phone available
  - b. Officers are notified to carry full equipment with them
  - c. 1-hour response capability
  - d. No alcohol consumption
  - e. All vehicles are serviced and ready
3. Level II Emergency Recall
  - a. Department personnel will be placed on 12-hour shifts
  - b. Shifts will consist of 0600 – 1800 hours and 1800 – 0600 hours
  - c. Each rotation will have a Sergeant in command.
4. Emergency Mobilization
  - a. Should emergency mobilization be required all personnel summoned to report to work will report in full uniform to the police department unless otherwise directed. All emergency equipment is stored at that location and will be issued as needed for any operation.

## G. Patrol Division Uniform

1. Class A “Parade Dress” consists of the following components:
  - a. Long sleeve uniform shirt
  - b. Tie
  - c. Badge
  - d. Name plate
  - e. Service/proficiency/award bars
  - f. Collar/sleeve rank insignia or collar pins
  - g. Trousers
  - h. Socks
  - i. Dress shoes/boots
  - j. Duty gear rig containing ONLY the following equipment
    - i. Inner belt
    - ii. Outer belt
    - iii. Holster
    - iv. Duty weapon
    - v. Double magazine holder with loaded magazines

- 
- vi. Handcuff case with handcuffs
  - vii. Radio holder with portable radio and shoulder microphone
  - viii. ASP baton and holder
  - ix. Any specialized items established for a specific ceremony or event and as approved by the Chief of Police Services or designee in charge of the ceremony or event.
  - k. In the event of inclement weather
    - i. Rain gear
2. "Class B "Duty Dress" consists of the following components:
- a. Seasonally approved uniform shirt
  - b. Badge
  - c. Name plate
  - d. Collar/sleeve rank insignia or collar pins
  - e. Dark blue, black, or white T-shirt or turtleneck
  - f. Uniform Trousers
  - g. Socks
  - h. Black Shoes/Boots
  - i. Duty gear rig containing the following equipment
    - i. Inner belt
    - ii. Outer belt
    - iii. Holster
    - iv. Duty Weapon
    - v. Double magazine holder with loaded magazines
    - vi. Handcuff case with handcuffs
    - vii. Radio holder with portable radio and shoulder microphone
    - viii. ASP baton with holder
    - ix. Mini flashlight holder with flashlight (optional)
  - j. Foul weather gear (if needed)
    - i. Wind breaker
    - ii. Rain coat
    - iii. Turtle neck
    - iv. Insulated Gloves if needed
    - v. Toboggan
  - k. Additional items may be worn, with written permission of the Chief of Police.
3. Class C "Work/Special Duty Dress" consists of the following components:
- a. Clothing appropriate for the type of special duty assigned while maintaining a professional representation for the department, unless in an undercover capacity.
4. The "Class B" uniform is worn daily during the performance of assigned duties by all police members, except those whose duties necessitate more traditional business attire or by members whose duty requires concealing the police identity from immediate sight, such as administrative or investigative assignments.

5. Off duty employment dress assignments require the use of plain clothes and is approved by the Chief of Police or his designee. No city equipment is authorized to be utilized for off duty private employment.
6. Each officer ensures that their equipment is kept in a state of repair and readiness
7. The replacement of the departmentally issued duty gear is the responsibility of the department.

### **III. ADMINISTRATIVE REQUIREMENTS**

#### **A. Calls for Service**

Members of the Patrol Division shall be responsible to respond to calls for service without delay to prevent injury, protect persons and property, and provide solutions to problems occurring in their respective district assignments.

#### **B. Multiple Officer Calls for Service**

1. Communication Personnel should dispatch the appropriate number of personnel or units to a specific call in order to accomplish the objective of the call for service.
2. Administrative, investigative, and other appropriate departmental personnel not generally assigned to patrol may also be contacted and requested to provide emergency assistance when necessary.
3. Number of Personnel Utilized
  - a. The specific number of personnel necessary to accomplish the objective of a specific call for service varies with the type and scope of the call.
  - b. While some police service calls can be addressed with a single officer, others may take multiple officers. Personnel shall utilize proper judgment in determining the appropriate number of personnel based on the available information and conditions existing at the time, and in accordance with the provisions contained herein.

#### **C. Radio Communications**

1. The department utilizes a plain English language description of call and activities to ensure clear understanding. 10-codes may be used in radio communications, but plain language is strongly encouraged. The department utilizes a standard phonetics code supplied to each new officer during their FTO training process.

#### **D. Portable Radio Usage**

1. Officers are issued portable radios. Officers are to carry the radios on their equipment belt while on duty. Officers may choose to utilize a shoulder microphone.
2. Portable radios will not be turned on in lieu of checking out with communications, When officers are out of their assigned unit they are required to check out with the dispatcher.

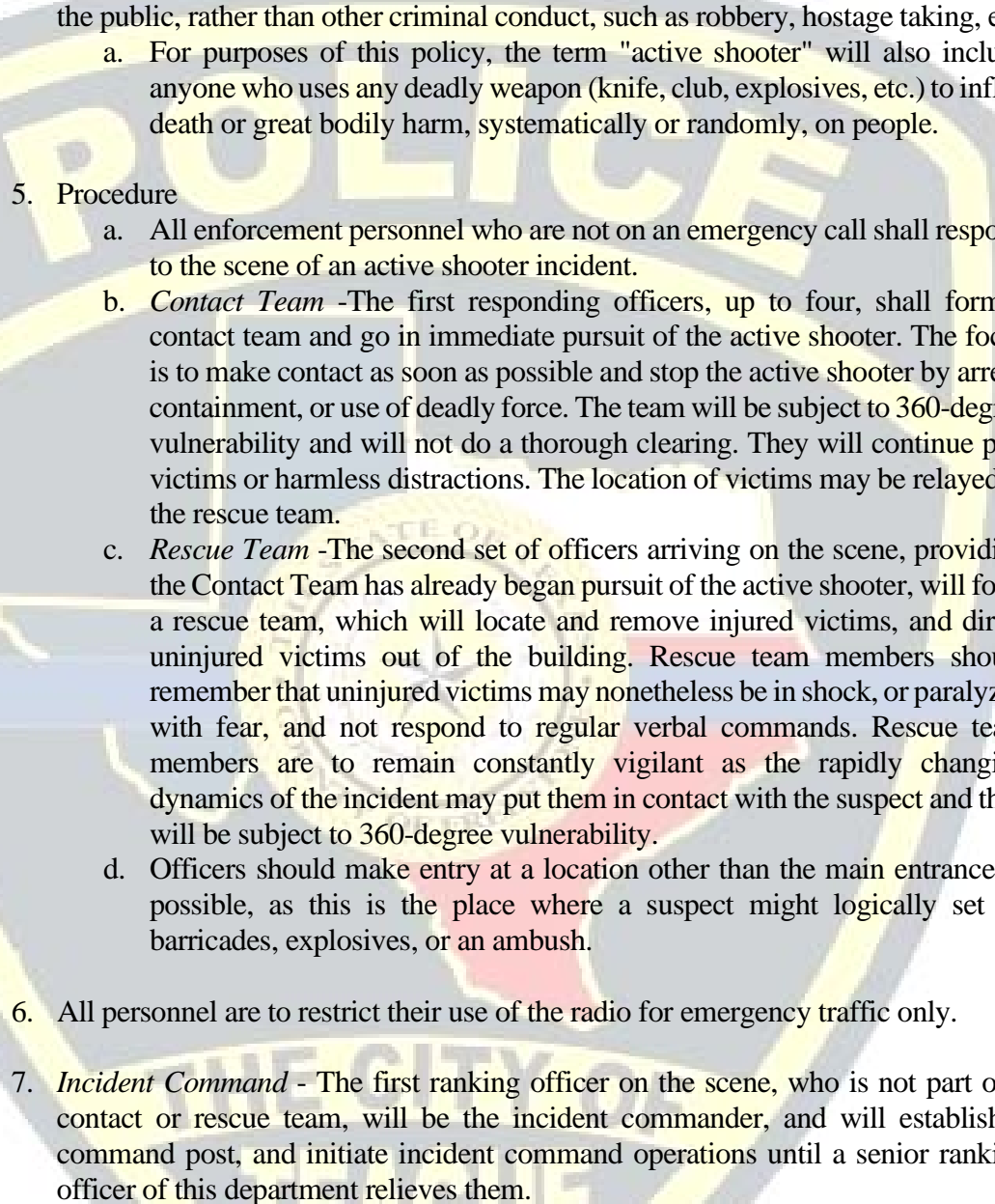
#### E. Report Writing

1. Officers are to complete detailed reports indicating the facts and circumstances of their investigation in an Offense/Incident Reports. Such reports should be concise and factual.
2. Officers should document calls that do not necessitate the need for an official report in their call for service module, when the call is completed.
3. Reports are to be completed prior to the end of the officer's tour of duty. If this cannot be accomplished, the officer's immediate supervisor is to be notified, who makes the decision if the completion of the report can be delayed.
4. At no time are reports to be delayed involving in custody arrests.

### **IV. PATROL FIELD TACTICS AND OPERATIONAL PROCEDURES**

#### A. Active Shooter Incident

1. It is the policy of this department to protect life by any legal means possible. Officers responding to an active shooter incident shall accomplish this goal by immediately using any legal means at their disposal to contact the active shooter and stop them. This may include arrest, containment, or use of deadly force.
2. The philosophy driving this policy recognizes that the active shooter must be stopped before he can destroy any more innocent lives. This shall be the duty and responsibility of the initial responding officers, and they shall use all legal means to accomplish it. The prioritization of activities, in their order of importance IS:
  - a. Stop the active shooter
  - b. Rescue the victims
  - c. Provide medical assistance
  - d. Preserve the crime scene.
3. While it is important to provide medical treatment to the wounded, it is our duty as law enforcement officers to first protect all innocent life by stopping the actions of the active shooter.

- 
4. An Active Shooter is defined as one or more subjects who participate in a random or systematic shooting spree, demonstrating their intent to continuously harm others. Their overriding object appears to be that of mass murder and terrorizing the public, rather than other criminal conduct, such as robbery, hostage taking, etc.
    - a. For purposes of this policy, the term "active shooter" will also include anyone who uses any deadly weapon (knife, club, explosives, etc.) to inflict death or great bodily harm, systematically or randomly, on people.
  5. Procedure
    - a. All enforcement personnel who are not on an emergency call shall respond to the scene of an active shooter incident.
    - b. *Contact Team* -The first responding officers, up to four, shall form a contact team and go in immediate pursuit of the active shooter. The focus is to make contact as soon as possible and stop the active shooter by arrest, containment, or use of deadly force. The team will be subject to 360-degree vulnerability and will not do a thorough clearing. They will continue past victims or harmless distractions. The location of victims may be relayed to the rescue team.
    - c. *Rescue Team* -The second set of officers arriving on the scene, providing the Contact Team has already began pursuit of the active shooter, will form a rescue team, which will locate and remove injured victims, and direct uninjured victims out of the building. Rescue team members should remember that uninjured victims may nonetheless be in shock, or paralyzed with fear, and not respond to regular verbal commands. Rescue team members are to remain constantly vigilant as the rapidly changing dynamics of the incident may put them in contact with the suspect and they will be subject to 360-degree vulnerability.
    - d. Officers should make entry at a location other than the main entrance, if possible, as this is the place where a suspect might logically set up barricades, explosives, or an ambush.
  6. All personnel are to restrict their use of the radio for emergency traffic only.
  7. *Incident Command* - The first ranking officer on the scene, who is not part of a contact or rescue team, will be the incident commander, and will establish a command post, and initiate incident command operations until a senior ranking officer of this department relieves them.

#### B. Building Searches

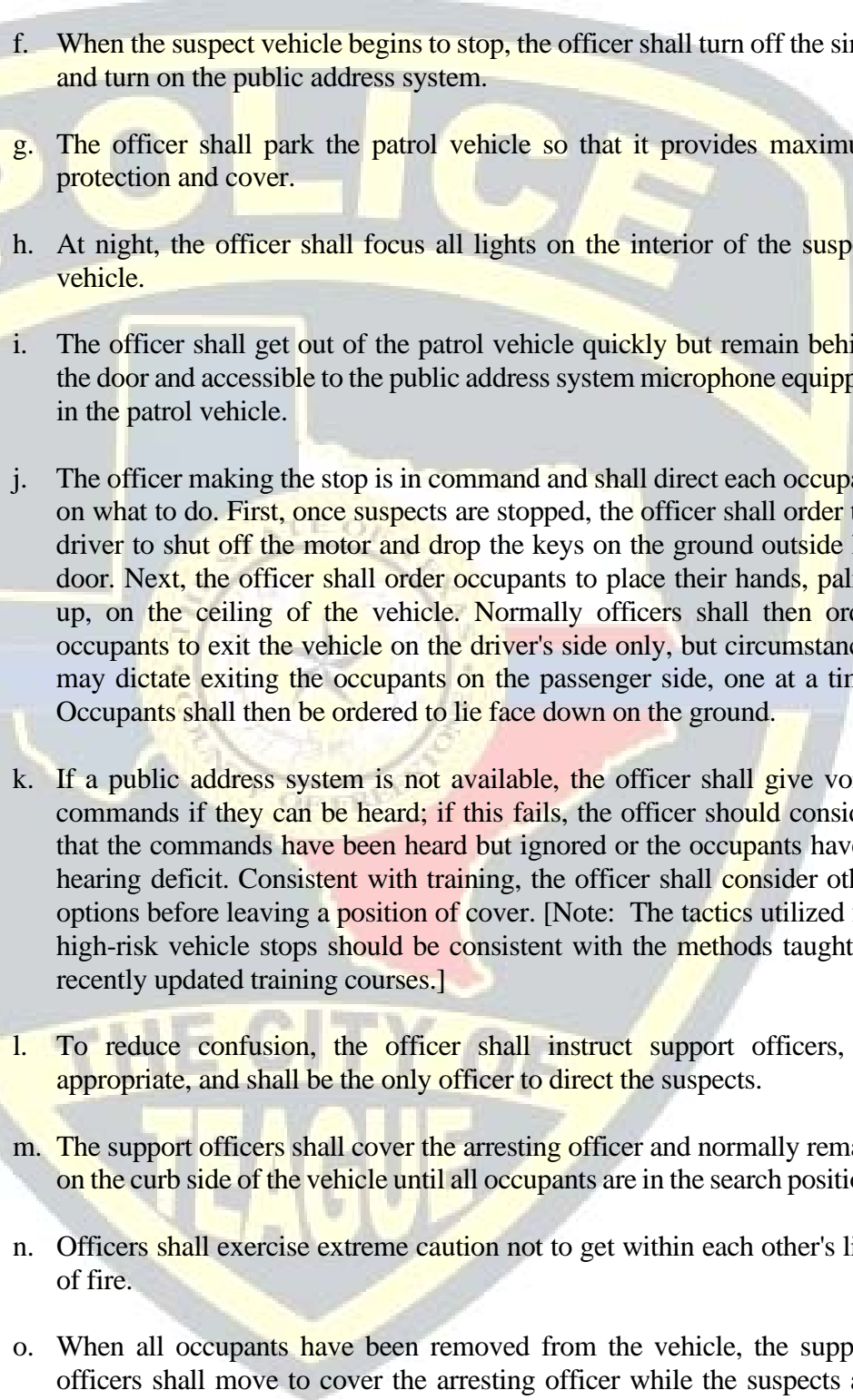
1. The officer in charge will formulate and direct a search plan based on the physical layout of the building.
2. Dispatch will be notified that officers are entering the building. Other officers should limit their radio conversation and officers entering the building should reduce the volume of their portable radios or use an earpiece.



3. Entry should never be made through small openings or windows, unless there is sufficient visual access to the inside of the building to provide cover for the entering officers. Entry normally should not be made by less than two officers.
4. Emergency conditions in which threat to life or property would result from a lack of immediate action on the part of the responding officer would, of course, require only that officer to act as quickly and safely as the situation dictates,
5. Officers should locate the lights and illuminate the area to be searched as the search progresses, however avoid "back lighting" themselves.
6. Officers should determine how a suspect may go from one level to another and secure them. The building should be divided into sectors and search methodically, keeping officers abreast of each other. It is not advisable for officers to separate or lose sight of fellow officers.
7. Officers should anticipate ambush points and examine all possible hiding places, i.e., look up, check trash containers, air conditioning vents, etc.
8. Officers should contact the dispatcher and let others know the building is clear as soon as possible.

#### C. Felony Stop Procedures

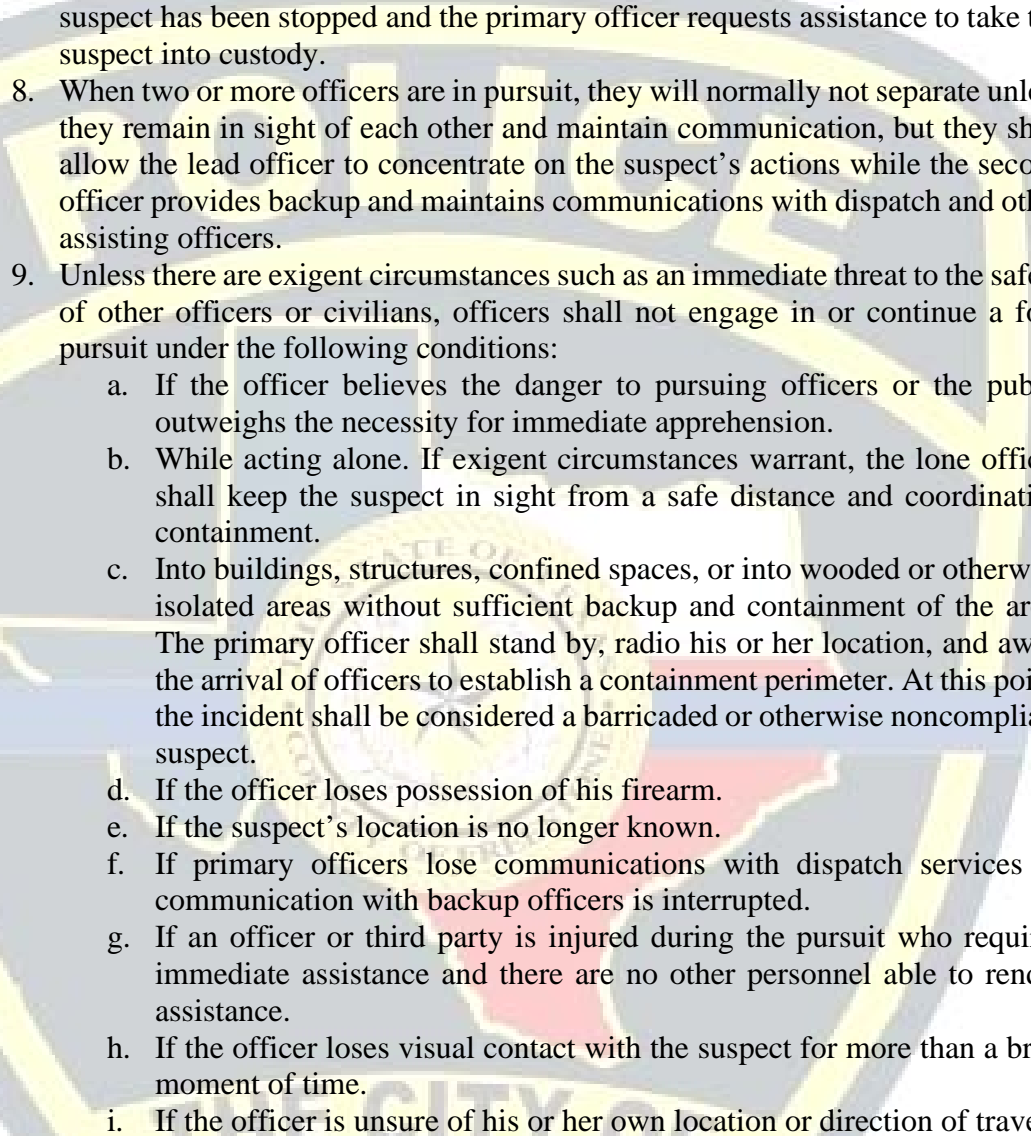
1. Special procedures shall be used in vehicle stops when the occupants are reasonably believed to be armed and dangerous. When an officer locates a vehicle driven by a known or suspected felon, the officer shall notify the dispatcher immediately of the suspect's location and give a thorough description of the vehicle and its occupants. The officer shall keep the suspect vehicle in view and request sufficient assistance in making the stop.
2. The officer shall keep support units informed of the suspect's location and direction of travel to aid their approach with minimal use of emergency equipment. The suspect vehicle shall not be stopped, unless absolutely necessary, until adequate support is available and in position. Circumstances may, however, dictate a one-officer felony vehicle stop.
3. The following procedures shall be used in effecting the stop:
  - a. The officer shall plan to stop the suspect vehicle in a location which presents minimal danger to the public.
  - b. When conditions are appropriate and support units available, the officer shall move into position to the rear of the suspect vehicle.
  - c. The officer shall signal the violator to stop, using all emergency equipment to warn other traffic.
  - d. The violator should be stopped on the extreme right side of the road, if circumstances permit.

- 
- e. If the violator is known to be armed and dangerous, the officer shall have his weapon easily accessible and ready for immediate use.
  - f. When the suspect vehicle begins to stop, the officer shall turn off the siren and turn on the public address system.
  - g. The officer shall park the patrol vehicle so that it provides maximum protection and cover.
  - h. At night, the officer shall focus all lights on the interior of the suspect vehicle.
  - i. The officer shall get out of the patrol vehicle quickly but remain behind the door and accessible to the public address system microphone equipped in the patrol vehicle.
  - j. The officer making the stop is in command and shall direct each occupant on what to do. First, once suspects are stopped, the officer shall order the driver to shut off the motor and drop the keys on the ground outside his door. Next, the officer shall order occupants to place their hands, palms up, on the ceiling of the vehicle. Normally officers shall then order occupants to exit the vehicle on the driver's side only, but circumstances may dictate exiting the occupants on the passenger side, one at a time. Occupants shall then be ordered to lie face down on the ground.
  - k. If a public address system is not available, the officer shall give voice commands if they can be heard; if this fails, the officer should consider that the commands have been heard but ignored or the occupants have a hearing deficit. Consistent with training, the officer shall consider other options before leaving a position of cover. [Note: The tactics utilized for high-risk vehicle stops should be consistent with the methods taught in recently updated training courses.]
  - l. To reduce confusion, the officer shall instruct support officers, as appropriate, and shall be the only officer to direct the suspects.
  - m. The support officers shall cover the arresting officer and normally remain on the curb side of the vehicle until all occupants are in the search position.
  - n. Officers shall exercise extreme caution not to get within each other's line of fire.
  - o. When all occupants have been removed from the vehicle, the support officers shall move to cover the arresting officer while the suspects are searched.

- p. All arrestees shall be searched and handcuffed before transportation.
- q. The cover officers should move forward and tactically clear the vehicle of any potentially concealed occupants.

#### D. Foot Pursuits

1. Although it is an officer's decision to initiate a stop, it is the suspect or violator who decides to precipitate a foot pursuit by fleeing. An officer's decision to pursue on foot shall be made with an awareness of and appreciation for the risk to which the officer and others will be exposed. No officer or supervisor shall be criticized or disciplined for a decision not to engage in a foot pursuit if, in the officer's assessment, the risk exceeds that which is reasonably acceptable.
2. Where necessary, an officer may pursue persons who he or she reasonably believes have committed an act that would warrant a stop, investigative detention, or arrest.
3. In deciding whether to initiate a pursuit, an officer shall consider the following alternatives to foot pursuit:
  - a. Containment of the area
  - b. Canine search
  - c. Saturation of the area with patrol personnel
4. In deciding whether to initiate or continue a foot pursuit, officers shall also consider risk factors whenever officers are:
  - a. acting alone,
  - b. in an unfamiliar area,
  - c. in an area that is hostile, such as a notorious drug trafficking location,
  - d. pursuing suspects who are known to be or suspected of being armed,
  - e. unable to obtain backup in a timely manner,
  - f. not in adequate physical condition to conduct a foot pursuit,
  - g. unable to establish and maintain contact with the communications center, or
  - h. pursuing in inclement weather, darkness, or reduced visibility conditions.
5. Officers initiating foot pursuits shall be in field command and shall bear operational responsibility for the foot pursuit unless circumstances dictate otherwise or until relieved by a supervisor. Pursuing officers are reminded that voice transmissions while running and in other field tactical situations may be difficult to understand and may have to be repeated.
6. The officer initiating a foot pursuit shall, as soon as practical, provide the following information to Communications:
  - a. Unit identifier
  - b. Reason for the foot pursuit
  - c. Officer location and direction of pursuit
  - d. Number of suspects and description
  - e. Whether or not the suspect(s) is armed
  - f. Location to which assisting officers are to respond

- 
- g. Location, if required, of any perimeter
  - 7. Assisting officers should immediately attempt to contain the pursued suspect. Such officers shall not respond to the primary officer's location unless the suspect has been stopped and the primary officer requests assistance to take the suspect into custody.
  - 8. When two or more officers are in pursuit, they will normally not separate unless they remain in sight of each other and maintain communication, but they shall allow the lead officer to concentrate on the suspect's actions while the second officer provides backup and maintains communications with dispatch and other assisting officers.
  - 9. Unless there are exigent circumstances such as an immediate threat to the safety of other officers or civilians, officers shall not engage in or continue a foot pursuit under the following conditions:
    - a. If the officer believes the danger to pursuing officers or the public outweighs the necessity for immediate apprehension.
    - b. While acting alone. If exigent circumstances warrant, the lone officer shall keep the suspect in sight from a safe distance and coordinating containment.
    - c. Into buildings, structures, confined spaces, or into wooded or otherwise isolated areas without sufficient backup and containment of the area. The primary officer shall stand by, radio his or her location, and await the arrival of officers to establish a containment perimeter. At this point, the incident shall be considered a barricaded or otherwise noncompliant suspect.
    - d. If the officer loses possession of his firearm.
    - e. If the suspect's location is no longer known.
    - f. If primary officers lose communications with dispatch services or communication with backup officers is interrupted.
    - g. If an officer or third party is injured during the pursuit who requires immediate assistance and there are no other personnel able to render assistance.
    - h. If the officer loses visual contact with the suspect for more than a brief moment of time.
    - i. If the officer is unsure of his or her own location or direction of travel

#### E. In-Progress Calls for Service

1. In progress calls demand three primary considerations. First to ensure the greatest level of safety available to all officers concerned with the call. Second, to contain the scene to prevent the escape of suspects; and third, to preserve the scene for all evidence.
2. The following are general guidelines for the handling of the majority of in progress calls:
  - a. The responding unit should go to the site of the premises where the case is most likely occurring.

- b. If, possible, officers should position their vehicle short of the scene to avoid showing your presence and position.
- c. Take appropriate time to size up the situation and formulate a plan, and to advise your cover officer.
- d. On armed robbery calls, for the safety of the victim and bystanders, arrests can best be affected outside the building.

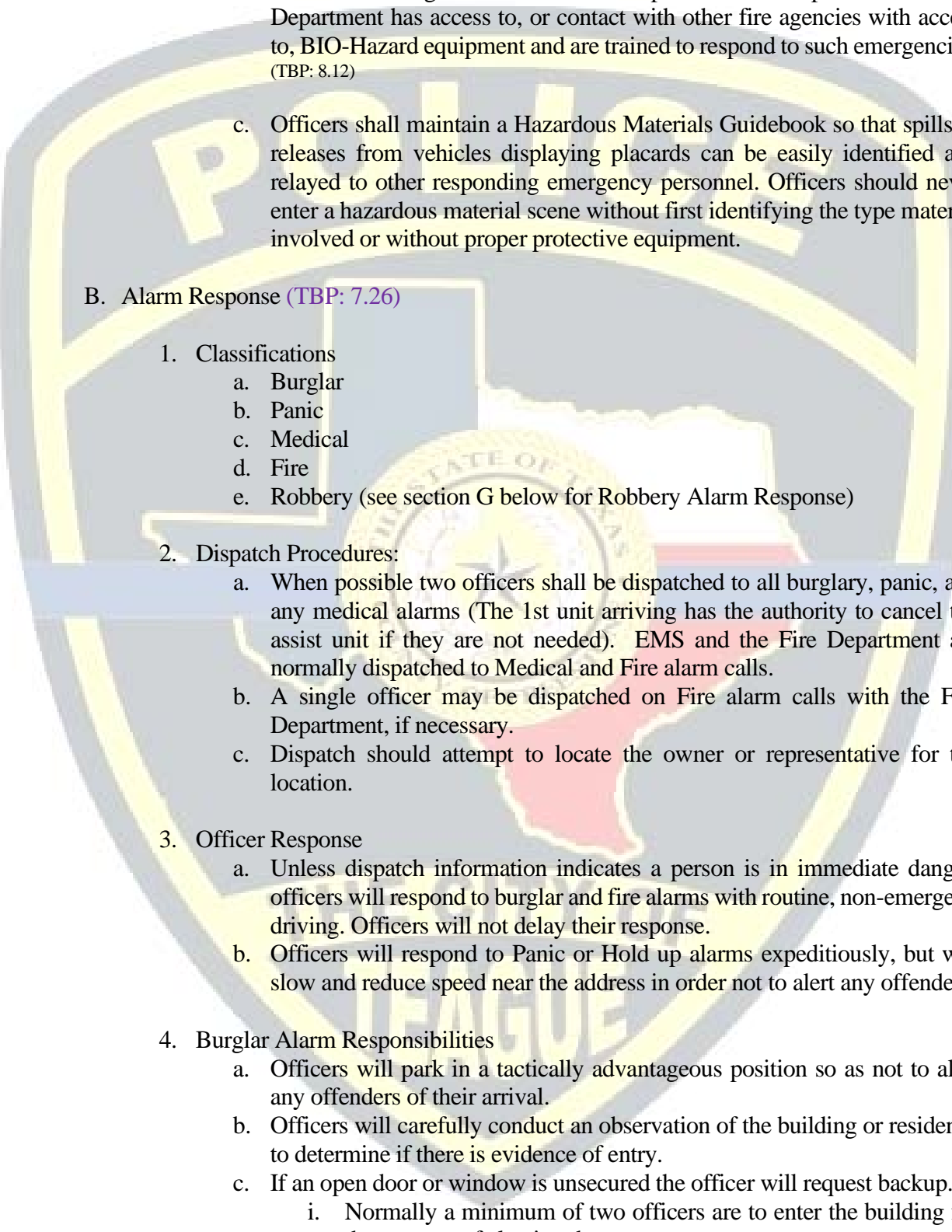
#### F. Adverse Weather Response

1. In the event of severe weather such as a thunderstorms passing through the area with damaging hail, high surface winds, and extremely heavy rain which reduces visibility or endangers personnel or vehicles, all units not on a call will immediately seek shelter at any protected area.
2. In the event of loss of traffic control devices due to a power outage, officers shall monitor the situation for dangerous traffic situations. TXDOT will be contacted for a state highway. For city intersections officers will direct traffic at the intersection only when conditions require. Public works may be contacted to erect temporary traffic control devices in lieu of officers directing traffic.
3. Officers should monitor low water crossings for flooding and notify appropriate personnel to assist in erecting barricades to restrict traffic through those areas. Officers should also monitor other roads for debris causing an impediment to vehicular traffic and request appropriate assistance to clear such obstructions.

### V. FIELD PROCEDURES FOR SPECIFIC INCIDENTS

#### A. Accident Investigation

1. Members of the Patrol Division respond to reports of all traffic accidents resulting in injury or damage if the accident occurred on public property.
2. Private Property Accidents (Restricted Access) Private property accidents may, but are not required to, be investigated. In the event of substantial damage, injury, or death officers shall initiate an accident investigation. Parking lots, for the purpose of accident reporting, are considered private property.
3. Enforcement Action
  - a. Unless there are extenuating circumstances patrol officers shall issue citations for traffic and equipment violations determined, during their investigation of the accident.
4. Hazardous Material Involvement
  - a. In the event of Hazardous Material involvement a perimeter is established around the accident site, limiting access ONLY to responding emergency personnel.

- 
- b. In the event of a large hazardous material spill or release, officers will contact the Teague Volunteer Fire Department for response. The Fire Department has access to, or contact with other fire agencies with access to, BIO-Hazard equipment and are trained to respond to such emergencies. (TBP: 8.12)
  - c. Officers shall maintain a Hazardous Materials Guidebook so that spills or releases from vehicles displaying placards can be easily identified and relayed to other responding emergency personnel. Officers should never enter a hazardous material scene without first identifying the type material involved or without proper protective equipment.

## B. Alarm Response (TBP: 7.26)

### 1. Classifications

- a. Burglar
- b. Panic
- c. Medical
- d. Fire
- e. Robbery (see section G below for Robbery Alarm Response)

### 2. Dispatch Procedures:

- a. When possible two officers shall be dispatched to all burglary, panic, and any medical alarms (The 1st unit arriving has the authority to cancel the assist unit if they are not needed). EMS and the Fire Department are normally dispatched to Medical and Fire alarm calls.
- b. A single officer may be dispatched on Fire alarm calls with the Fire Department, if necessary.
- c. Dispatch should attempt to locate the owner or representative for the location.

### 3. Officer Response

- a. Unless dispatch information indicates a person is in immediate danger, officers will respond to burglar and fire alarms with routine, non-emergent, driving. Officers will not delay their response.
- b. Officers will respond to Panic or Hold up alarms expeditiously, but will slow and reduce speed near the address in order not to alert any offenders.

### 4. Burglar Alarm Responsibilities

- a. Officers will park in a tactically advantageous position so as not to alert any offenders of their arrival.
- b. Officers will carefully conduct an observation of the building or residence to determine if there is evidence of entry.
- c. If an open door or window is unsecured the officer will request backup.
  - i. Normally a minimum of two officers are to enter the building for the purpose of clearing the structure.

- ii. Officers shall advise dispatch and responding officers of the location of the open door or window, and when officers are entering the building.
- d. The responding officer will determine if a representative of the household should respond.
- e. Officers will stand by if advised that a representative is enroute to their location. If a representative or owner is not enroute, the location should be secured to the extent possible.
- f. Prior to clearing the scene, the primary officer will leave their business card in a conspicuous place, if the officers entered the location without an owner present.

#### 5. Panic Alarm Responsibilities

- a. Officers will park in a tactically advantageous position so as not to alert any offenders of their arrival. Sometimes medical alarms have been used in cases of domestic disturbances and officers should be alert to this possibility.
- b. The responding officer may have the dispatcher attempt to contact the residence by phone prior to their approach.
- c. If contact is made, communications should request the complainant meet the officer outside.
- d. If contact is not made, the officers should carefully approach the location and attempt to determine if anything is wrong. A supervisor should be contacted for further instructions.

#### 6. Medical Alarm Responsibilities

- a. Officers will park in a tactically advantageous position so as not to alert any offenders of their arrival. Some medical alarms have been used in cases of domestic disturbances and officers should be alert to this possibility.
- b. Officers should carefully approach the location and determine if a medical emergency exists. If a medical emergency exists, the officer should assist the complainant to the level of their training and ability while ensuring EMS is responding and assist them in easily locating the victim.

#### 7. Fire Alarm Responsibilities

- a. When arriving prior to the Fire Department, officers will park in a position that will not hamper fire department access to the location or any fire hydrant.
- b. When arriving prior to the Fire Department the officer will advise the dispatcher if any evidence of fire is showing (flames, smoke, and evacuated facility, etc.).
- c. If no evidence of fire is present and the Fire Department has not yet arrived, the officer shall attempt to locate the fire alarm location and responsible party.

- d. If the officer arrives after the Fire Department, he/she will consult with the Fire Department officer in charge for their needs such as crowd control and traffic management.

#### C. Arson Investigations

1. The investigation of arson is primarily the responsibility of the Police Department. It is the responsibility of the Fire Department to determine cause of origin. The Police Department will assist in the Fire Department in any way possible.
2. In some cases, especially where a fire has been started and the fire has either gone out or has been extinguished, the complainant may notify the Police Department rather than the Fire Department.
3. Patrol Officers will secure the scene and have the communications notify the City Fire Marshal for an investigator to be sent to the scene.
4. In all cases where a Fire Investigator is not sent to the scene, the responsibility of the investigation lies with the Police Department. In such cases a supervisor will be contacted.
5. The patrol officer initially assigned the complaint shall be responsible for the initial case report.

#### D. Assault Investigations

1. The primary officer assigned is responsible for the initial investigation. The officer shall control the scene to ensure all evidence is protected. The officer should first attempt to establish if the victim requires medical attention, and if so, request an ambulance. The officer shall then decide whether an actual offense has taken place. The officer's investigation should include but is not limited to the following.
  - a. Interview with the victim
  - b. Interview all witnesses.
  - c. Identity of all individuals at the location at the time of the offense.
  - d. Identify the suspect (to include name and address
  - e. Relationship of the victim and suspect (family member, etc.)
  - f. If possible, interview the suspect.
  - g. Description as to the method of assaults (hands, weapon, etc.)
  - h. Description of the injuries.
  - i. Description of the crime scene.
  - j. Photographs of injuries, scene, and evidence
  - k. If the assault is aggravated in nature a supervisor should be notified.

#### E. Auto Theft (UUV) Investigations

1. The responding officer is responsible for the preliminary investigation. The officer should establish that an actual offense has taken place. The officer's investigation should include, but is not limited to, the following:
  - a. Accurate description of the vehicle make, model, year, and color.
  - b. Registration information including the vehicle identification number.



- c. Any distinguishing information (bumper stickers, decals, body damage or any other identifiable details).
  - d. Lien holder information and determine if the payments are up to date or if there is the possibility of a repossession.
  - e. How many sets of keys, and where they are located.
  - f. Amount of fuel in the vehicle.
2. If a stolen vehicle is located, the officer shall follow policy and procedure regarding taking possession of the vehicle and notifying the originating agency or owner. The originating agency will be responsible for placing a hold on recovered vehicles. If recovered vehicle originated from Teague Police Department, then supervisor approval is needed to place a hold on that vehicle. Officers will complete a supplemental report to the original case, noting recovery of the vehicle and documenting the location and recovering agency.

F. Bank Alarm/ Robbery Response (TBP: 7.26)

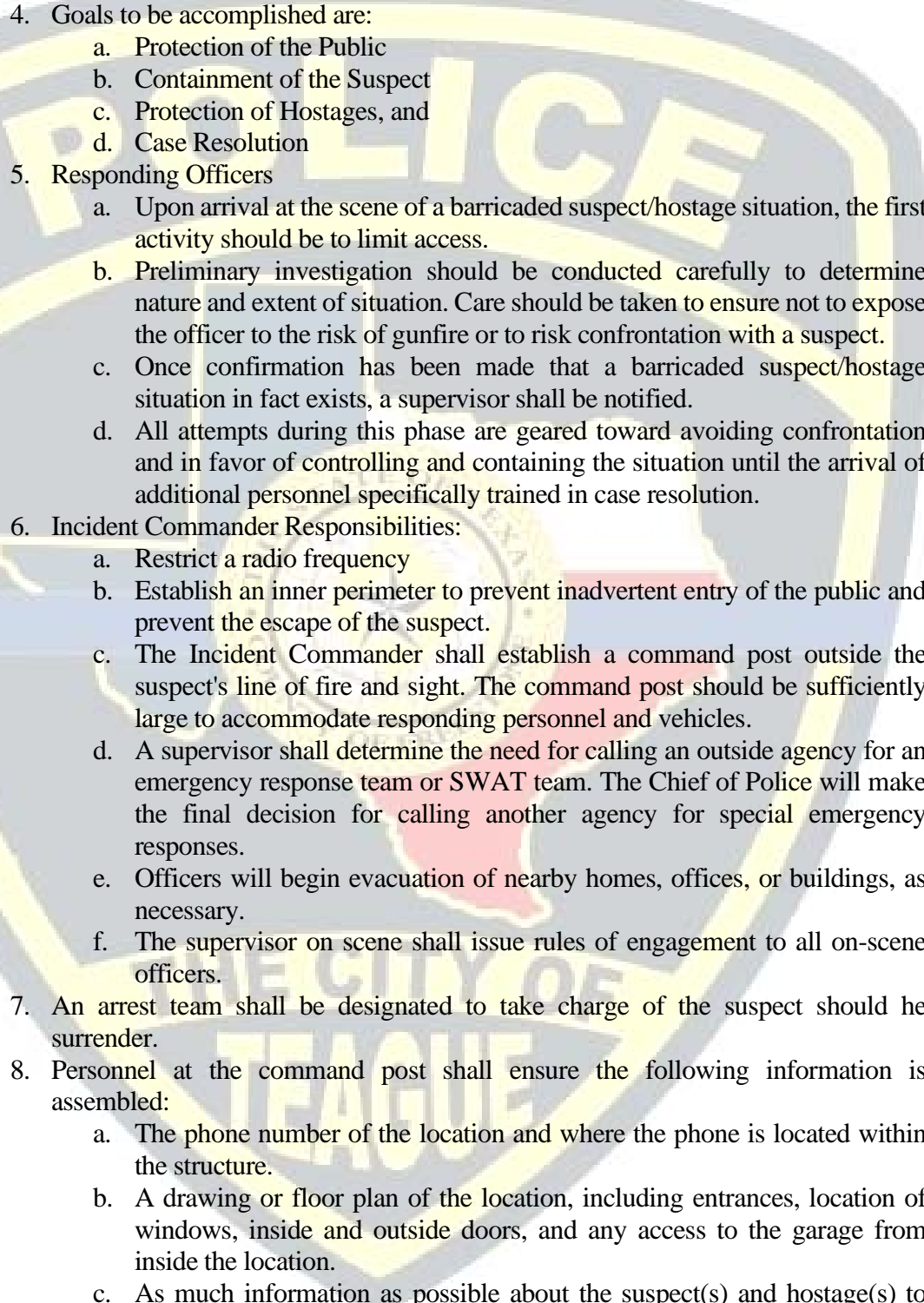
1. Upon receipt of a financial institution alarm, normally a minimum of two unmarked patrol units should be dispatched, if available.
2. If the robbery notification is received by telephone, a complete description of the perpetrators should be obtained from the caller, along with as much additional information as possible; particularly whether the perpetrator is at the scene and if not, his direction and mode of travel and a complete description of any vehicle involved.
3. If the robbery notification at other locations is made by alarm, the dispatcher should not attempt to contact the institution or residence in order to determine the validity of the alarm until officers have given notice that they are in position at the location.
  - a. If the dispatcher is subsequently notified that the alarm is false prior to the officer's arrival, they should advise the caller that police units are responding and;
    - i. obtain the identity of and maintain contact with the caller
    - ii. verify the false alarm with a key employee of the establishment (e.g., manager or head teller) and advise them they will need to exit the location to meet the responding officers.
    - iii. obtain a physical description of the key employee and provide responding officers with the description and the fact that they will meet them outside as required.
4. Responding officers shall use appropriate vehicular warning devices when approaching the scene, but the siren will not be used within the hearing range of the reported robbery.
5. Responding units to the scene should be observant of any suspicious vehicles leaving the scene as well as other vehicles or persons outside the facility who may be serving as lookouts, cover, or drivers for a robbery team.
6. The first unit on the scene shall serve as the primary unit until relieved by a supervisor. The first unit on the scene shall take a position that provides good

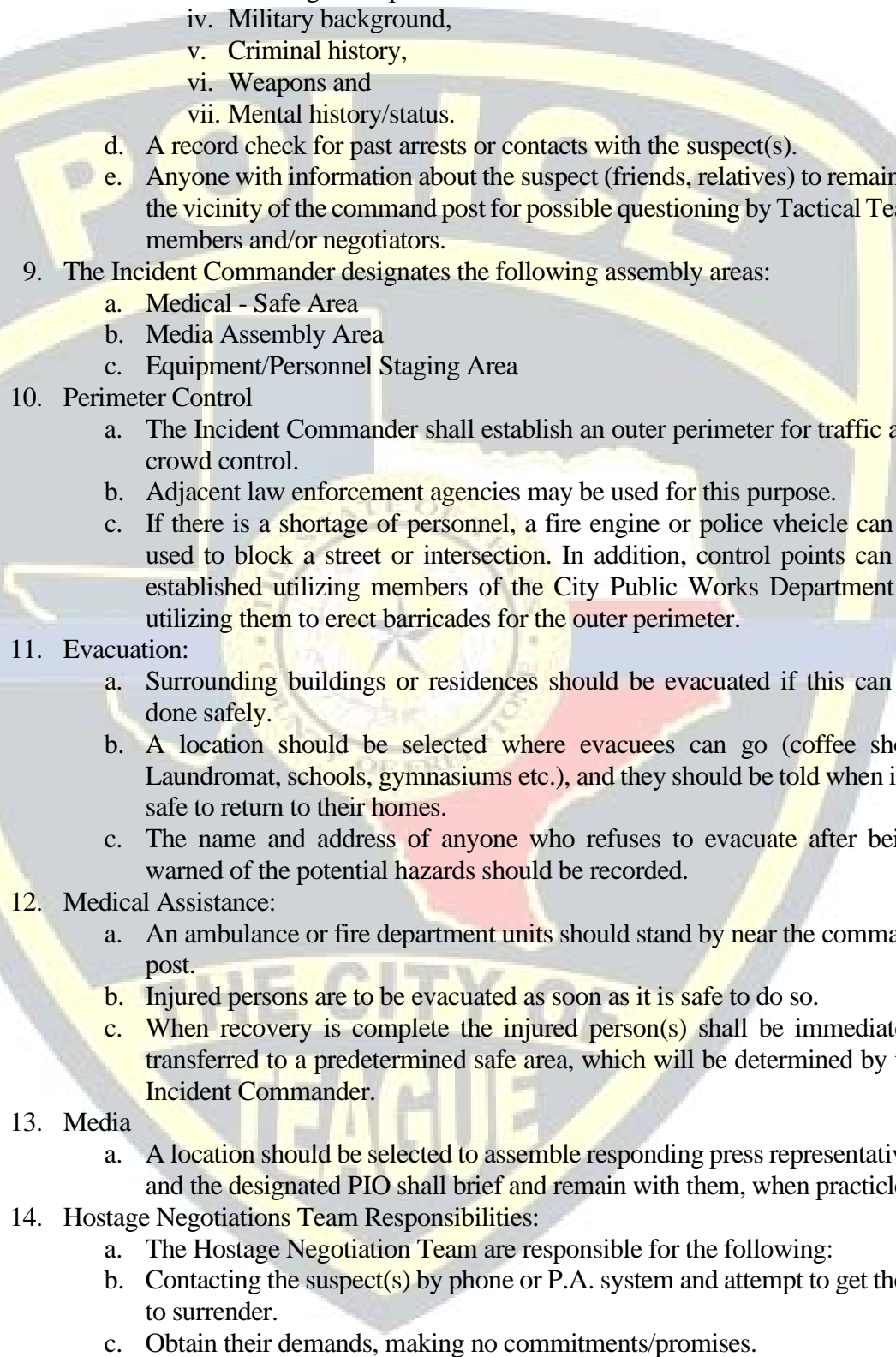
observation without being easily visible to those inside. The primary unit shall report on observable conditions at the location to the dispatcher but should not initially approach the location without appropriate support.

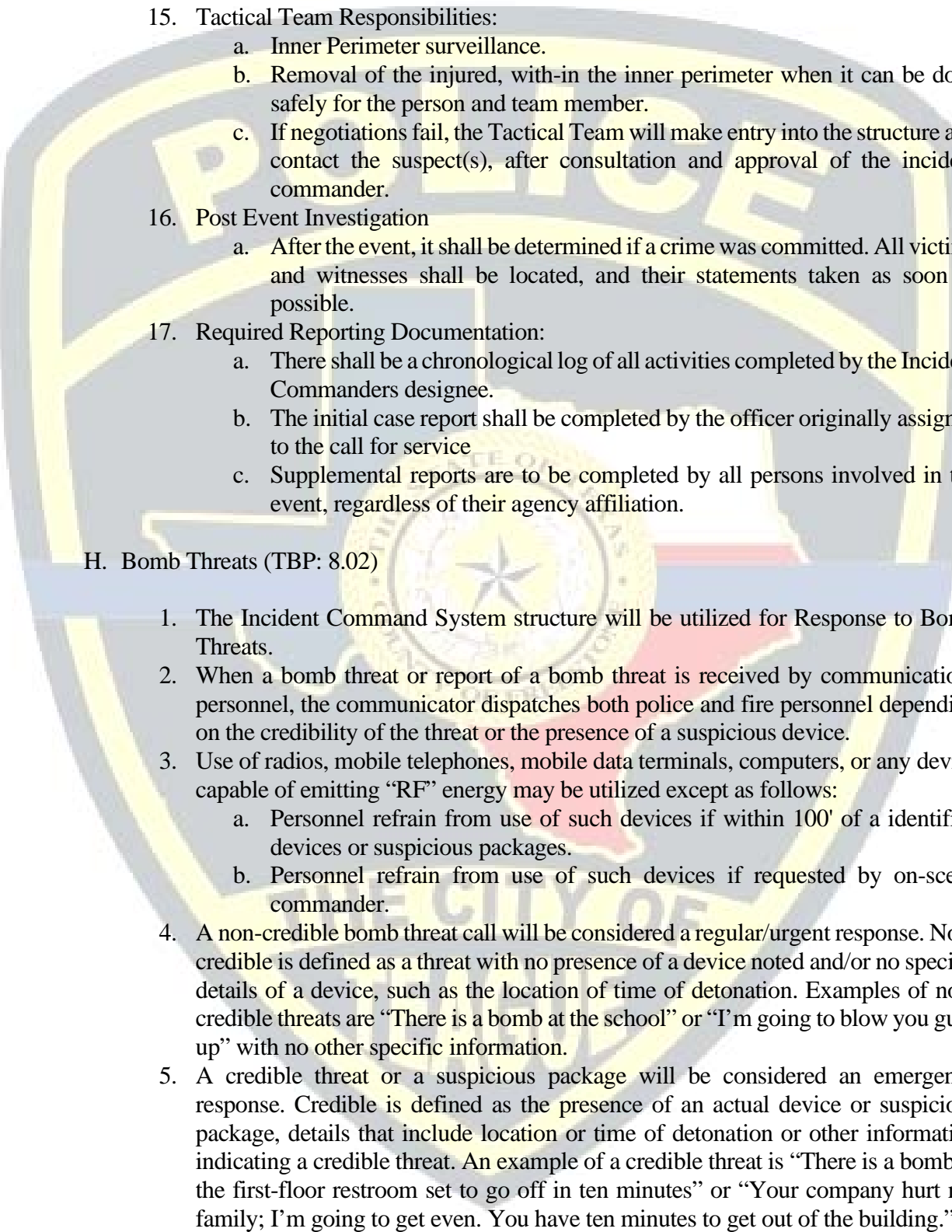
7. The primary and all subsequent units arriving at the robbery location shall report their arrival and position to the dispatcher. The primary unit or supervisory officer should direct responding units into positions that will establish a perimeter covering all exits and entrances.
8. Once the location perimeter has been established and no notice of a false alarm has been received, the primary unit on the scene shall determine whether the dispatcher shall telephone the location. If the call is made, the dispatcher should identify himself and inquire whether a robbery is in progress. If the call is not answered or a questionable response is provided to the inquiry, officers at the scene should be informed of these facts and told that a possible robbery is in progress.
9. If a robbery in progress is suspected, the primary unit or supervisory officer shall determine whether to request additional backup support from Freestone County Sheriff's Office.
10. Unless otherwise directed, officers shall wait until suspects have exited the location before attempting apprehension. This helps to avoid the development of a hostage situation.
11. Once perpetrators have left the location, the crime scene shall be secured by officers in preparation for processing by crime scene units and federal agents.
12. If a robbery has been committed and the perpetrators have left the scene, the primary unit should begin preparation of the initial report by identifying witnesses, caring for any injured parties, protecting the crime scene and obtaining necessary information regarding the perpetrators for supplemental broadcast. Remaining units should initiate the search for suspects on likely escape routes, being alert to unusual activities and circumstances.
13. If the dispatcher notifies officers that they have been in contact with an employee of the establishment or resident and there does not appear to be a robbery in progress, officers shall determine the identity and description of the individual and wait for him to exit the building and approach the officers. Officers shall accompany the employee into the establishment to verify the situation and shall notify dispatch once the verification is complete.
14. If the alarm is received after business hours and the establishment is not occupied, responding officers shall assume positions in the front and rear of the building and jointly conduct an inspection of the location for signs of forced entry. If signs of forced entry exist, officers shall follow procedures for conducting a building search. If the building is secure, dispatch shall be notified and requested to contact the owner or the establishment's designated contact person to meet them at the location.

#### G. Barricaded Subjects/Hostage Investigations (TBP: 8.01)

1. Events involving hostage or barricaded suspects will be addressed in accordance with the Incident Command System.

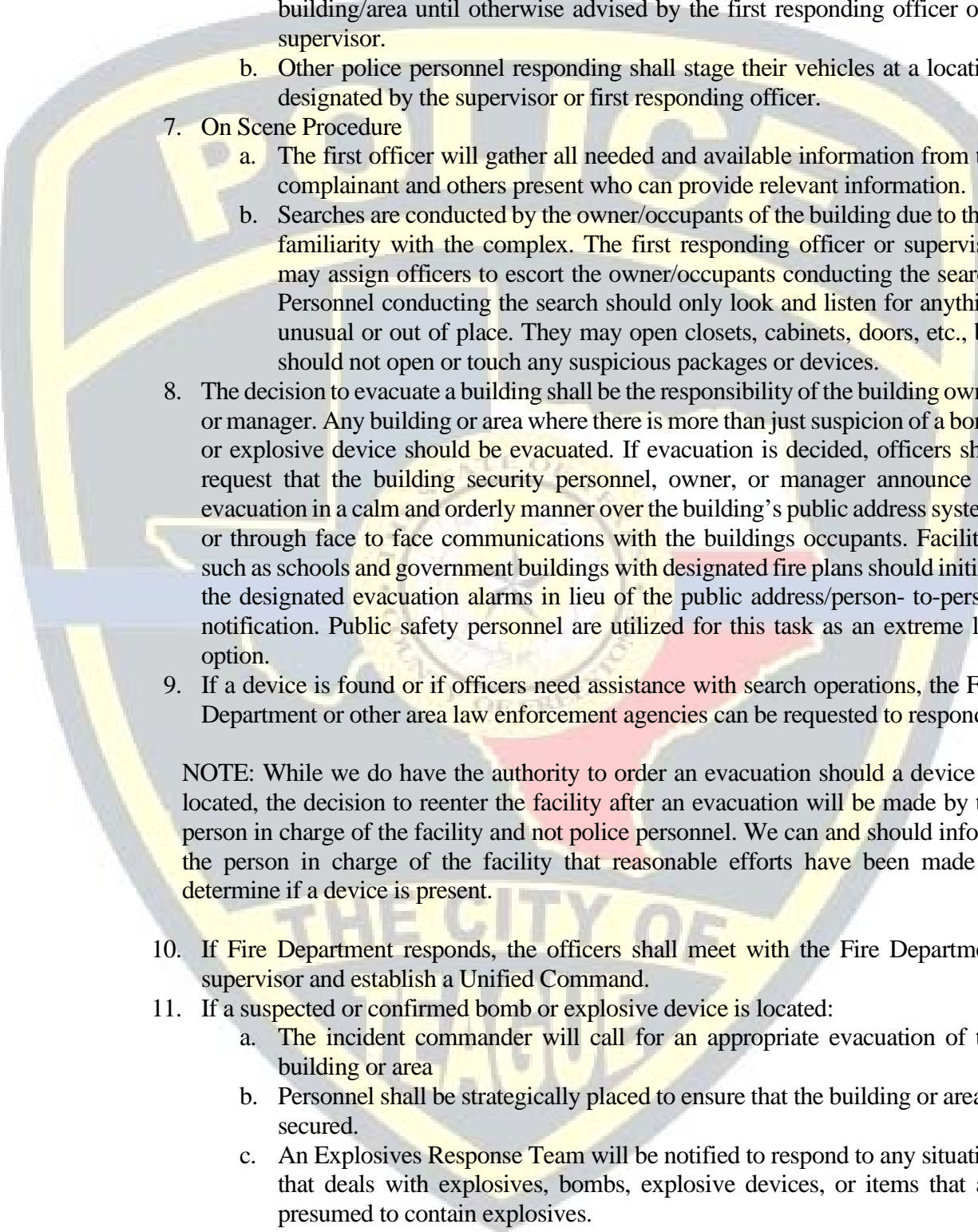
- 
2. A supervisor will be dispatched on any Barricaded suspect or Hostage situation.
  3. The responding supervisor will assume the duties of the Incident Commander until relieved by a higher-ranking officer of this department.
  4. Goals to be accomplished are:
    - a. Protection of the Public
    - b. Containment of the Suspect
    - c. Protection of Hostages, and
    - d. Case Resolution
  5. Responding Officers
    - a. Upon arrival at the scene of a barricaded suspect/hostage situation, the first activity should be to limit access.
    - b. Preliminary investigation should be conducted carefully to determine nature and extent of situation. Care should be taken to ensure not to expose the officer to the risk of gunfire or to risk confrontation with a suspect.
    - c. Once confirmation has been made that a barricaded suspect/hostage situation in fact exists, a supervisor shall be notified.
    - d. All attempts during this phase are geared toward avoiding confrontation and in favor of controlling and containing the situation until the arrival of additional personnel specifically trained in case resolution.
  6. Incident Commander Responsibilities:
    - a. Restrict a radio frequency
    - b. Establish an inner perimeter to prevent inadvertent entry of the public and prevent the escape of the suspect.
    - c. The Incident Commander shall establish a command post outside the suspect's line of fire and sight. The command post should be sufficiently large to accommodate responding personnel and vehicles.
    - d. A supervisor shall determine the need for calling an outside agency for an emergency response team or SWAT team. The Chief of Police will make the final decision for calling another agency for special emergency responses.
    - e. Officers will begin evacuation of nearby homes, offices, or buildings, as necessary.
    - f. The supervisor on scene shall issue rules of engagement to all on-scene officers.
  7. An arrest team shall be designated to take charge of the suspect should he surrender.
  8. Personnel at the command post shall ensure the following information is assembled:
    - a. The phone number of the location and where the phone is located within the structure.
    - b. A drawing or floor plan of the location, including entrances, location of windows, inside and outside doors, and any access to the garage from inside the location.
    - c. As much information as possible about the suspect(s) and hostage(s) to include:
      - i. Name,

- 
- ii. Physical description,
  - iii. Clothing description,
  - iv. Military background,
  - v. Criminal history,
  - vi. Weapons and
  - vii. Mental history/status.
- d. A record check for past arrests or contacts with the suspect(s).
  - e. Anyone with information about the suspect (friends, relatives) to remain in the vicinity of the command post for possible questioning by Tactical Team members and/or negotiators.
9. The Incident Commander designates the following assembly areas:
- a. Medical - Safe Area
  - b. Media Assembly Area
  - c. Equipment/Personnel Staging Area
10. Perimeter Control
- a. The Incident Commander shall establish an outer perimeter for traffic and crowd control.
  - b. Adjacent law enforcement agencies may be used for this purpose.
  - c. If there is a shortage of personnel, a fire engine or police vehicle can be used to block a street or intersection. In addition, control points can be established utilizing members of the City Public Works Department or utilizing them to erect barricades for the outer perimeter.
11. Evacuation:
- a. Surrounding buildings or residences should be evacuated if this can be done safely.
  - b. A location should be selected where evacuees can go (coffee shop, Laundromat, schools, gymnasiums etc.), and they should be told when it is safe to return to their homes.
  - c. The name and address of anyone who refuses to evacuate after being warned of the potential hazards should be recorded.
12. Medical Assistance:
- a. An ambulance or fire department units should stand by near the command post.
  - b. Injured persons are to be evacuated as soon as it is safe to do so.
  - c. When recovery is complete the injured person(s) shall be immediately transferred to a predetermined safe area, which will be determined by the Incident Commander.
13. Media
- a. A location should be selected to assemble responding press representatives and the designated PIO shall brief and remain with them, when practicable.
14. Hostage Negotiations Team Responsibilities:
- a. The Hostage Negotiation Team are responsible for the following:
  - b. Contacting the suspect(s) by phone or P.A. system and attempt to get them to surrender.
  - c. Obtain their demands, making no commitments/promises.
  - d. Do not allow the suspect(s) and hostage(s) to leave the location.

- 
- e. Do not allow friends, relatives, or other interested persons to enter the location.
15. Tactical Team Responsibilities:
    - a. Inner Perimeter surveillance.
    - b. Removal of the injured, with-in the inner perimeter when it can be done safely for the person and team member.
    - c. If negotiations fail, the Tactical Team will make entry into the structure and contact the suspect(s), after consultation and approval of the incident commander.
  16. Post Event Investigation
    - a. After the event, it shall be determined if a crime was committed. All victims and witnesses shall be located, and their statements taken as soon as possible.
  17. Required Reporting Documentation:
    - a. There shall be a chronological log of all activities completed by the Incident Commanders designee.
    - b. The initial case report shall be completed by the officer originally assigned to the call for service
    - c. Supplemental reports are to be completed by all persons involved in the event, regardless of their agency affiliation.

#### H. Bomb Threats (TBP: 8.02)

1. The Incident Command System structure will be utilized for Response to Bomb Threats.
2. When a bomb threat or report of a bomb threat is received by communications personnel, the communicator dispatches both police and fire personnel depending on the credibility of the threat or the presence of a suspicious device.
3. Use of radios, mobile telephones, mobile data terminals, computers, or any device capable of emitting “RF” energy may be utilized except as follows:
  - a. Personnel refrain from use of such devices if within 100' of a identified devices or suspicious packages.
  - b. Personnel refrain from use of such devices if requested by on-scene commander.
4. A non-credible bomb threat call will be considered a regular/urgent response. Non-credible is defined as a threat with no presence of a device noted and/or no specific details of a device, such as the location of time of detonation. Examples of non-credible threats are “There is a bomb at the school” or “I’m going to blow you guys up” with no other specific information.
5. A credible threat or a suspicious package will be considered an emergency response. Credible is defined as the presence of an actual device or suspicious package, details that include location or time of detonation or other information indicating a credible threat. An example of a credible threat is “There is a bomb in the first-floor restroom set to go off in ten minutes” or “Your company hurt my family; I’m going to get even. You have ten minutes to get out of the building.”
6. Arrival on Scene

- 
- a. The first officer to arrive makes personal and immediate contact with the reportee. Other assigned officers shall stage away from the suspected building/area until otherwise advised by the first responding officer or a supervisor.
  - b. Other police personnel responding shall stage their vehicles at a location designated by the supervisor or first responding officer.
7. On Scene Procedure
- a. The first officer will gather all needed and available information from the complainant and others present who can provide relevant information.
  - b. Searches are conducted by the owner/occupants of the building due to their familiarity with the complex. The first responding officer or supervisor may assign officers to escort the owner/occupants conducting the search. Personnel conducting the search should only look and listen for anything unusual or out of place. They may open closets, cabinets, doors, etc., but should not open or touch any suspicious packages or devices.
8. The decision to evacuate a building shall be the responsibility of the building owner or manager. Any building or area where there is more than just suspicion of a bomb or explosive device should be evacuated. If evacuation is decided, officers shall request that the building security personnel, owner, or manager announce an evacuation in a calm and orderly manner over the building's public address system, or through face to face communications with the buildings occupants. Facilities such as schools and government buildings with designated fire plans should initiate the designated evacuation alarms in lieu of the public address/person- to-person notification. Public safety personnel are utilized for this task as an extreme last option.
9. If a device is found or if officers need assistance with search operations, the Fire Department or other area law enforcement agencies can be requested to respond.

NOTE: While we do have the authority to order an evacuation should a device be located, the decision to reenter the facility after an evacuation will be made by the person in charge of the facility and not police personnel. We can and should inform the person in charge of the facility that reasonable efforts have been made to determine if a device is present.

10. If Fire Department responds, the officers shall meet with the Fire Department supervisor and establish a Unified Command.
11. If a suspected or confirmed bomb or explosive device is located:
  - a. The incident commander will call for an appropriate evacuation of the building or area
  - b. Personnel shall be strategically placed to ensure that the building or area is secured.
  - c. An Explosives Response Team will be notified to respond to any situation that deals with explosives, bombs, explosive devices, or items that are presumed to contain explosives.

- d. In the event an Explosives Response Team is unavailable, an alternate Explosive Ordinance Disposal Team may be contacted from another agency or federal services.

#### I. Burglary Investigations

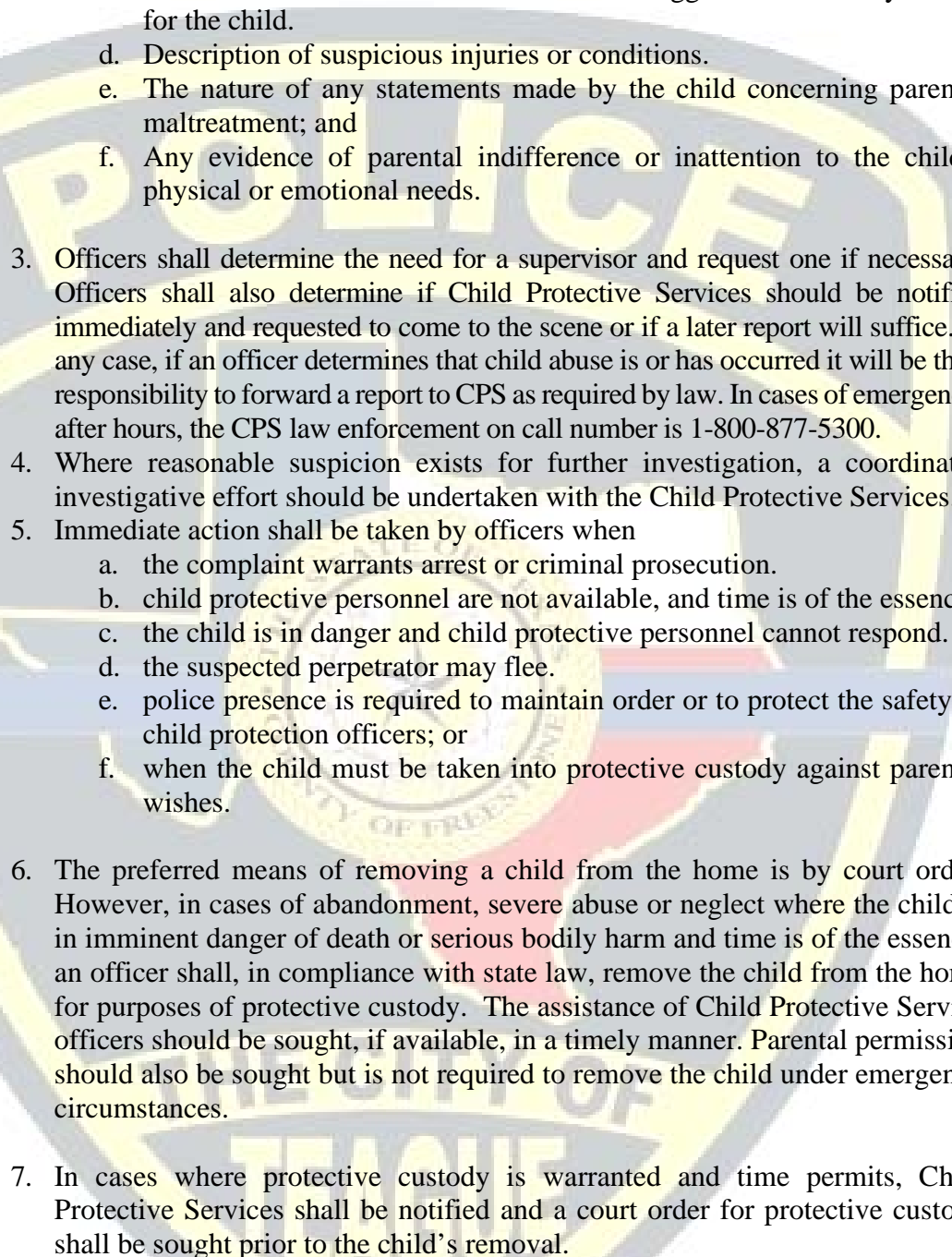
1. The primary responding officer is responsible for the initial investigation. The officer will control the scene to ensure that all evidence is protected. The officer shall attempt to establish that an actual offense has taken place. The investigation should include, but is not limited to the following:
  - a. the point of entry (including the method of entry)
  - b. the point of exit.
  - c. point(s) of impact (what the suspect did while on the scene)
  - d. determination of missing and damaged property.
  - e. interview of all witnesses
  - f. interview with the neighbors or area businesses
2. The officer shall determine the need for crime scene processing services to respond and assist in processing.
3. The officer, through consultation with a supervisor, may call additional officers to assist with gathering statements from witnesses and victims.

#### J. Burglary in Progress Calls for Service

1. On all burglary in progress calls a minimum of two (2) officers should be dispatched to the scene.
2. Upon the officers' arrival an exterior perimeter is established.
3. Once a perimeter is established, additional officers may search the building. Buildings are not to be searched by a lone officer, unless no other option is available.
4. If the owner of the property is present, neither they nor any other person are permitted to assist with the search until the building has been cleared. Civilians shall be staged away from the building in a place of safety.

#### K. Child Abuse

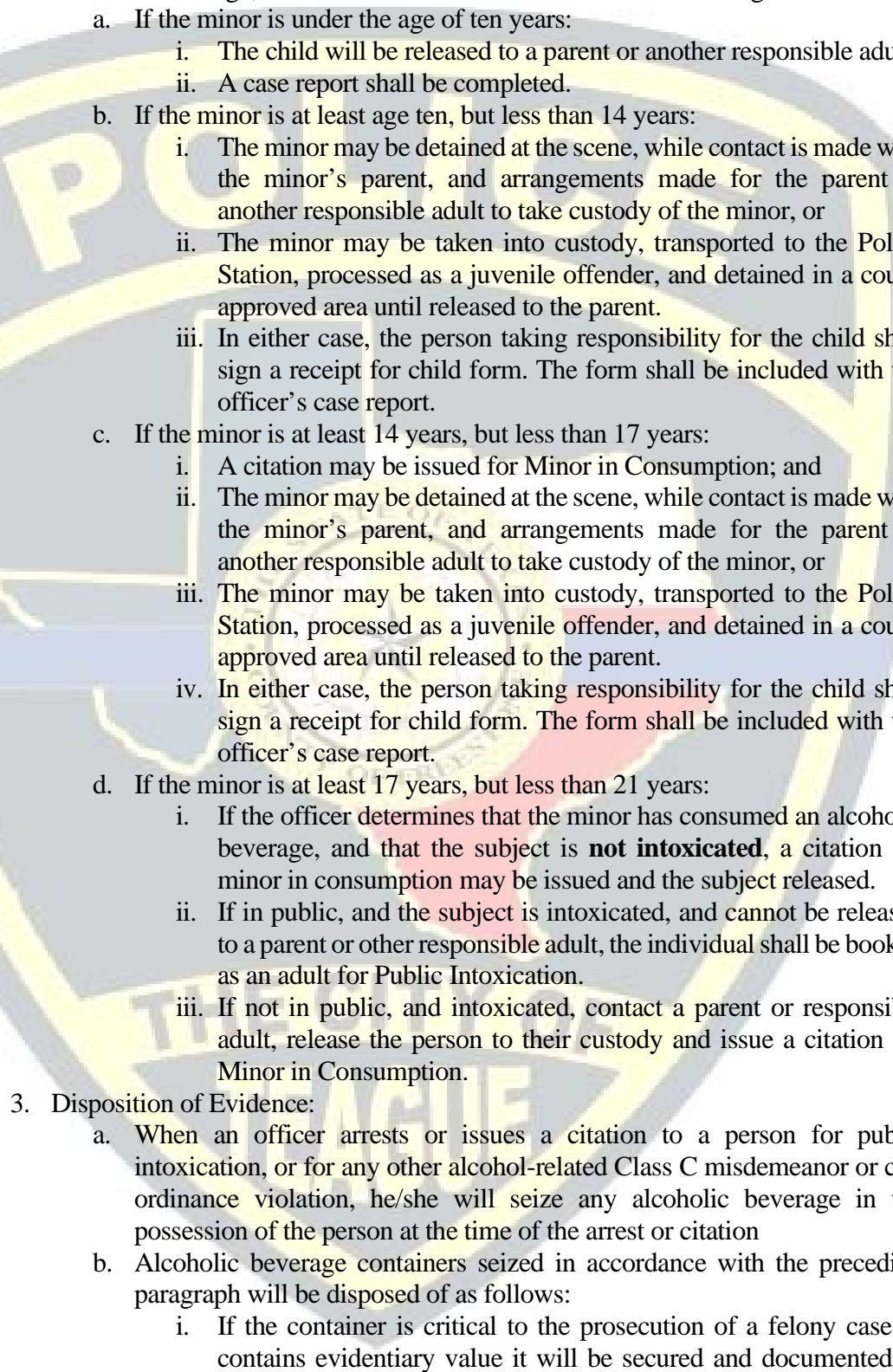
1. The primary officer dispatched is responsible for the initial investigation. State law requires that instances or suspected child abuse or neglect be reported by public and private officials such as physicians, dentists, school employees, clergymen and others. Officers shall record and respond to all reports of child abuse, neglect, and abandonment irrespective of the source or method of reporting.
2. A preliminary interview will be conducted with the reporting individual, when known, to determine the basis for the report, to include determination of such factors as:
  - a. The physical condition of the child.
  - b. A description of the abusive or neglectful behavior.

- 
- c. Evidence of parental disabilities such as alcoholism, drug abuse, mental illness or other factors that demonstrate or suggest their inability to care for the child.
      - d. Description of suspicious injuries or conditions.
      - e. The nature of any statements made by the child concerning parental maltreatment; and
      - f. Any evidence of parental indifference or inattention to the child's physical or emotional needs.
    3. Officers shall determine the need for a supervisor and request one if necessary. Officers shall also determine if Child Protective Services should be notified immediately and requested to come to the scene or if a later report will suffice. In any case, if an officer determines that child abuse is or has occurred it will be their responsibility to forward a report to CPS as required by law. In cases of emergency, after hours, the CPS law enforcement on call number is 1-800-877-5300.
    4. Where reasonable suspicion exists for further investigation, a coordinated investigative effort should be undertaken with the Child Protective Services.
    5. Immediate action shall be taken by officers when
      - a. the complaint warrants arrest or criminal prosecution.
      - b. child protective personnel are not available, and time is of the essence.
      - c. the child is in danger and child protective personnel cannot respond.
      - d. the suspected perpetrator may flee.
      - e. police presence is required to maintain order or to protect the safety of child protection officers; or
      - f. when the child must be taken into protective custody against parental wishes.
    6. The preferred means of removing a child from the home is by court order. However, in cases of abandonment, severe abuse or neglect where the child is in imminent danger of death or serious bodily harm and time is of the essence, an officer shall, in compliance with state law, remove the child from the home for purposes of protective custody. The assistance of Child Protective Service officers should be sought, if available, in a timely manner. Parental permission should also be sought but is not required to remove the child under emergency circumstances.
    7. In cases where protective custody is warranted and time permits, Child Protective Services shall be notified and a court order for protective custody shall be sought prior to the child's removal.

L. Consumption or possession of Alcohol by a Minor

1. Where a person is underage and suspected of having consumed an alcoholic beverage, and the officer believes the subject to be intoxicated, the officer should conduct standardized field sobriety tests, documenting the results in their case reports.

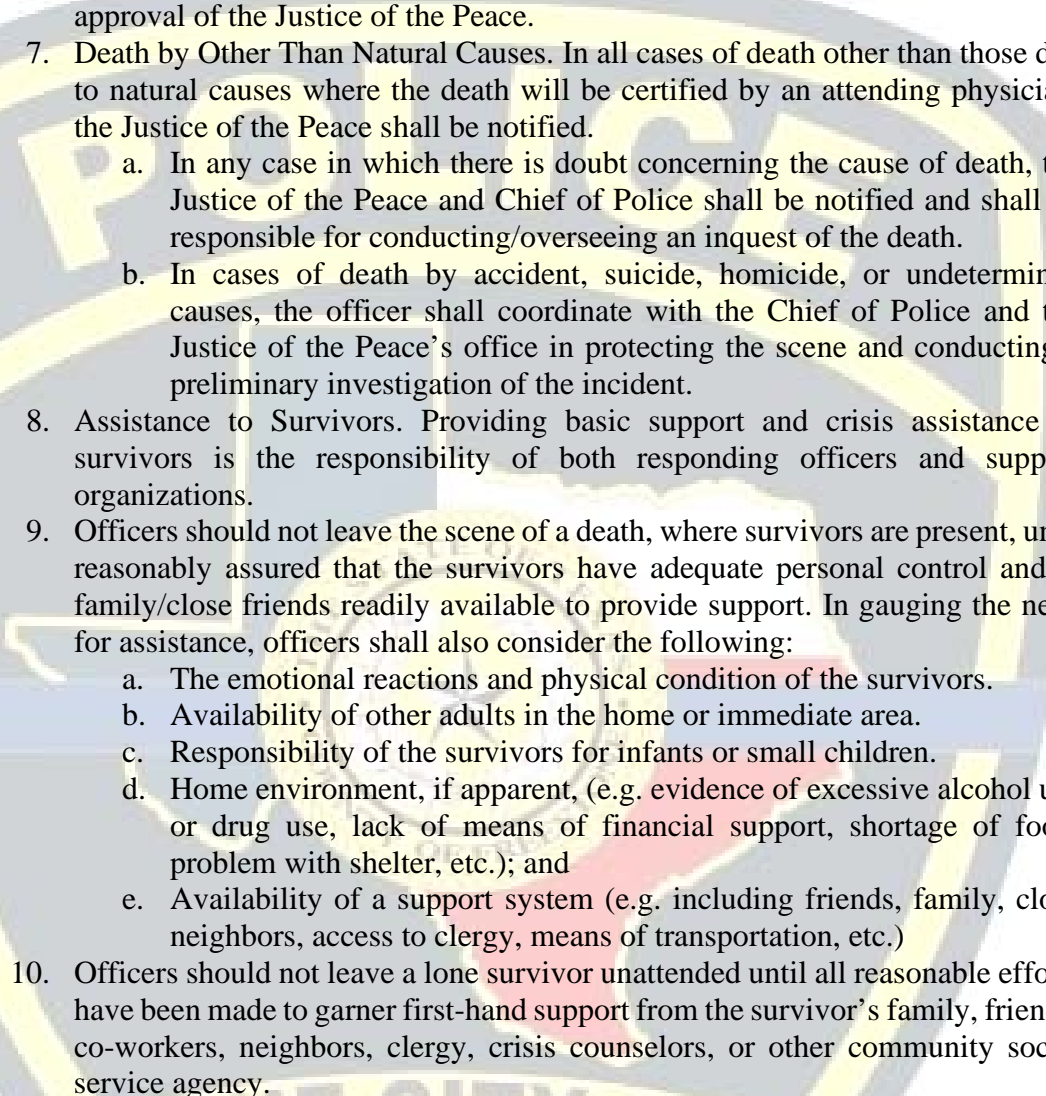


- 
2. When an officer determines that a person is underage and has consumed an alcoholic beverage, the officer shall undertake one of the following actions:
    - a. If the minor is under the age of ten years:
      - i. The child will be released to a parent or another responsible adult.
      - ii. A case report shall be completed.
    - b. If the minor is at least age ten, but less than 14 years:
      - i. The minor may be detained at the scene, while contact is made with the minor's parent, and arrangements made for the parent or another responsible adult to take custody of the minor, or
      - ii. The minor may be taken into custody, transported to the Police Station, processed as a juvenile offender, and detained in a court-approved area until released to the parent.
      - iii. In either case, the person taking responsibility for the child shall sign a receipt for child form. The form shall be included with the officer's case report.
    - c. If the minor is at least 14 years, but less than 17 years:
      - i. A citation may be issued for Minor in Consumption; and
      - ii. The minor may be detained at the scene, while contact is made with the minor's parent, and arrangements made for the parent or another responsible adult to take custody of the minor, or
      - iii. The minor may be taken into custody, transported to the Police Station, processed as a juvenile offender, and detained in a court-approved area until released to the parent.
      - iv. In either case, the person taking responsibility for the child shall sign a receipt for child form. The form shall be included with the officer's case report.
    - d. If the minor is at least 17 years, but less than 21 years:
      - i. If the officer determines that the minor has consumed an alcoholic beverage, and that the subject is **not intoxicated**, a citation for minor in consumption may be issued and the subject released.
      - ii. If in public, and the subject is intoxicated, and cannot be released to a parent or other responsible adult, the individual shall be booked as an adult for Public Intoxication.
      - iii. If not in public, and intoxicated, contact a parent or responsible adult, release the person to their custody and issue a citation for Minor in Consumption.
  3. Disposition of Evidence:
    - a. When an officer arrests or issues a citation to a person for public intoxication, or for any other alcohol-related Class C misdemeanor or city ordinance violation, he/she will seize any alcoholic beverage in the possession of the person at the time of the arrest or citation
    - b. Alcoholic beverage containers seized in accordance with the preceding paragraph will be disposed of as follows:
      - i. If the container is critical to the prosecution of a felony case or contains evidentiary value it will be secured and documented as would any other evidence

- ii. In misdemeanor cases each container of alcohol, whether opened or unopened, will be poured out and the container properly discarded, after photographs have been attained.
- iii. Destruction of any alcoholic beverage at the scene is done within view of the officer's patrol units video camera or body camera and included with the case report.

#### M. Death Investigations

1. Deceased persons or persons near death may be encountered in response to a wide variety of calls for service. Officers who encounter such situations shall, in order of importance, based on the circumstances, perform the following:
  - a. Identify and arrest any perpetrator(s) if present, and determination that a crime has been committed.
  - b. Ensure officer safety and the safety of others by safeguarding any weapons at the scene.
  - c. Administer emergency first aid if necessary and/or summon emergency medical personnel.
2. Death can only be determined in an official capacity by a physician. However, in cases involving unmistakable evidence of death (e.g., the presence of lividity or rigor mortis), emergency medical personnel need not be summoned.
  - a. If the officer determines that the person is dead, the factors surrounding that determination shall be entered into the officer's report.
  - b. Officers shall resolve any doubt concerning the life or death of a subject by summoning appropriate medical assistance.
3. The officer shall isolate and protect the crime scene from any intrusion by non-essential personnel including officers not directly involved in the crime scene investigation.
4. The officer shall notify communications of the circumstances and any additional personnel as needed. If the death is perceived to be a homicide or potential homicide or the result of accident or suicide, the Chief of Police shall also be summoned. The Chief of Police will determine the need for outside agency investigative services to assist with the investigation.
5. The officer shall observe and note pertinent information at the scene.
  - a. Record the nature of any physical modifications to the crime scene as the result of intervention by emergency medical personnel or others.
  - b. Record in a crime scene log the identity of any persons who were present at or who entered the crime scene.
  - c. Identify witnesses and record basic information regarding the event. Ask witnesses to remain, if possible. If not possible, determine their identity and how they can be contacted by investigators and have them provide a written statement, before leaving the scene.
  - d. Identify and ensure that any suspects do not leave. Responding officers may conduct basic, preliminary questioning of a suspect or witness, but should normally defer interviews to investigators.

- 
6. Bodies shall not be moved unless located in a spot that is deemed untenable (e.g., in open view of the public) and only under conditions that do not require a magistrates' response. In all other cases, bodies may not be moved without approval of the Justice of the Peace.
  7. Death by Other Than Natural Causes. In all cases of death other than those due to natural causes where the death will be certified by an attending physician, the Justice of the Peace shall be notified.
    - a. In any case in which there is doubt concerning the cause of death, the Justice of the Peace and Chief of Police shall be notified and shall be responsible for conducting/overseeing an inquest of the death.
    - b. In cases of death by accident, suicide, homicide, or undetermined causes, the officer shall coordinate with the Chief of Police and the Justice of the Peace's office in protecting the scene and conducting a preliminary investigation of the incident.
  8. Assistance to Survivors. Providing basic support and crisis assistance to survivors is the responsibility of both responding officers and support organizations.
  9. Officers should not leave the scene of a death, where survivors are present, until reasonably assured that the survivors have adequate personal control and/or family/close friends readily available to provide support. In gauging the need for assistance, officers shall also consider the following:
    - a. The emotional reactions and physical condition of the survivors.
    - b. Availability of other adults in the home or immediate area.
    - c. Responsibility of the survivors for infants or small children.
    - d. Home environment, if apparent, (e.g. evidence of excessive alcohol use or drug use, lack of means of financial support, shortage of food, problem with shelter, etc.); and
    - e. Availability of a support system (e.g. including friends, family, close neighbors, access to clergy, means of transportation, etc.)
  10. Officers should not leave a lone survivor unattended until all reasonable efforts have been made to garner first-hand support from the survivor's family, friends, co-workers, neighbors, clergy, crisis counselors, or other community social service agency.

#### N. Death Notifications

##### 1. Preparations

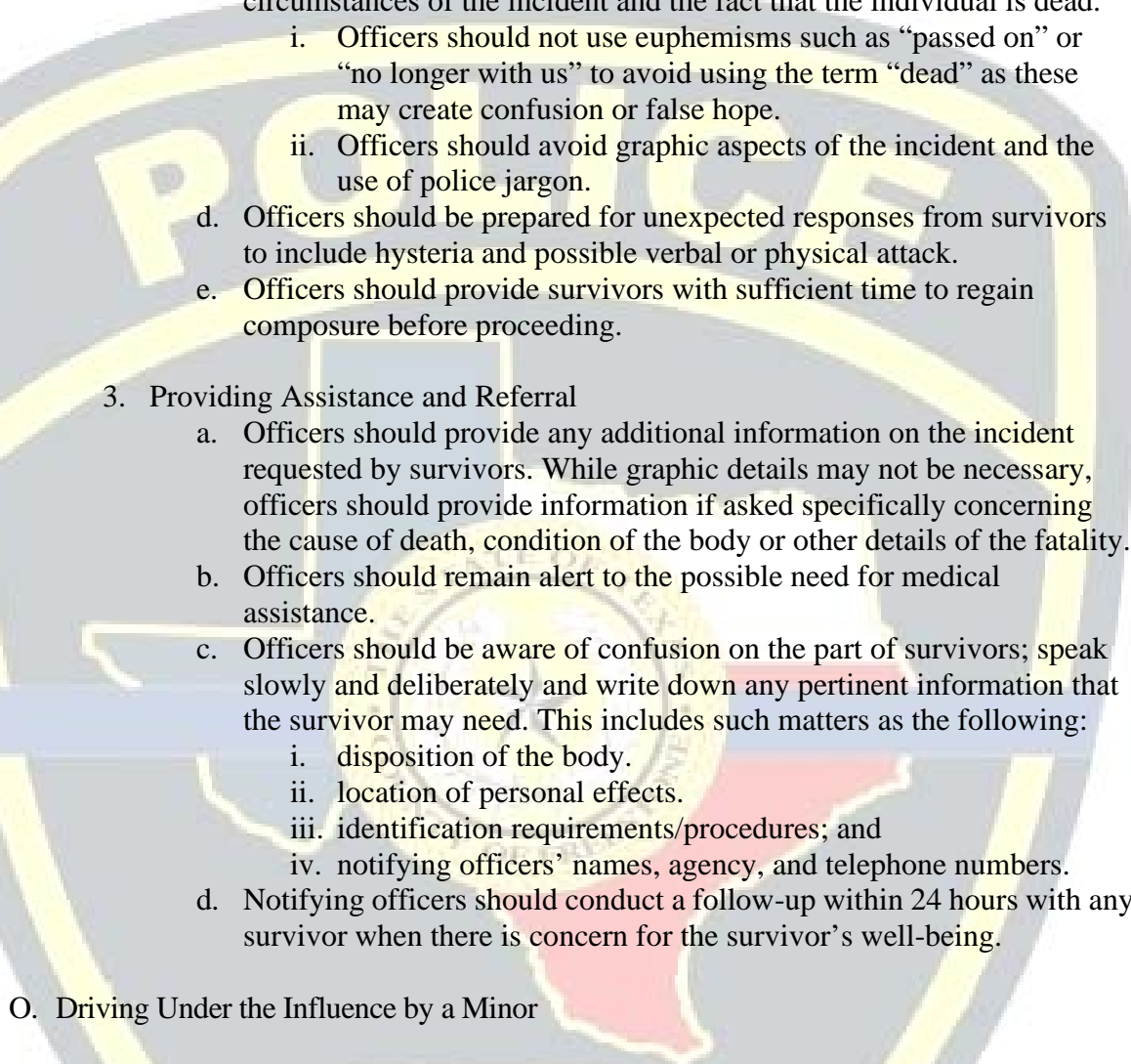
- a. All death notifications that are the responsibility of this agency shall be delivered in person unless the exigency of circumstances demands telephonic notification.
- b. Officers shall be prepared to and shall be provided adequate discretion to spend the necessary time with survivors to provide assistance as authorized by this standard operating procedure.
- c. Prior to contacting next of kin, notifying officers shall gather and familiarize themselves with essential details concerning the deceased,

to include full name, age, race and home address, as well as details of the death, location of the body/personal effects and other pertinent information. Officers shall identify the next of kin of the deceased for purposes of notification. Effort should be made to locate the closest relative starting with a spouse and followed by parents, brothers, or sisters, then children.

- d. Only where substantial delays would be required to contact next of kin should other relatives be contacted.
- e. Officers should contact a supervisor for guidance when in doubt concerning next of kin or delays in notification.
- f. Where another agency must be contacted to notify the next of kin, officers should
  - i. request that the notification be made in person, and
  - ii. request immediate verification when notification has been accomplished.
- g. Wherever possible, officers should gather available information concerning the survivors that may aid in the notification. This includes but is not limited to whether survivors are elderly, disabled, visually or hearing impaired, have medical problems or may not speak English. If possible, obtain the names of the survivor's closest relative, friend, family doctor and clergyman.
- h. Officers shall ensure that they have on hand a list of referral agencies that may be helpful and should leave this with survivors.
- i. Officers should, wherever reasonably possible, avoid using the name of the deceased over the radio prior to notification of immediate surviving relatives.
- j. Where possible, two officers (preferably a male and female team) should be assigned to a death notification when practical.
- k. Officers should request the assistance of clergy or local crisis intervention specialist where feasible and practical.
- l. Personal effects of the deceased shall not be delivered to survivors at the time of death notification.

## 2. Making Notification

- a. Upon arrival at the residence or place of business, officers shall do the following:
  - i. check the accuracy of the location.
  - ii. request to speak to the immediate survivor.
  - iii. identify themselves by name, rank, and departmental affiliation.
  - iv. verify the relationship of the survivor to the deceased; and
  - v. ask to move to a place of privacy.
- b. Every reasonable effort shall be made to make the death notification in the privacy of the survivor's home or in another location away from public scrutiny.

- 
- c. Officers should address the survivor(s) in a straightforward manner and use easy-to-understand language to briefly explain the circumstances of the incident and the fact that the individual is dead.
    - i. Officers should not use euphemisms such as “passed on” or “no longer with us” to avoid using the term “dead” as these may create confusion or false hope.
    - ii. Officers should avoid graphic aspects of the incident and the use of police jargon.
  - d. Officers should be prepared for unexpected responses from survivors to include hysteria and possible verbal or physical attack.
  - e. Officers should provide survivors with sufficient time to regain composure before proceeding.
3. Providing Assistance and Referral
- a. Officers should provide any additional information on the incident requested by survivors. While graphic details may not be necessary, officers should provide information if asked specifically concerning the cause of death, condition of the body or other details of the fatality.
  - b. Officers should remain alert to the possible need for medical assistance.
  - c. Officers should be aware of confusion on the part of survivors; speak slowly and deliberately and write down any pertinent information that the survivor may need. This includes such matters as the following:
    - i. disposition of the body.
    - ii. location of personal effects.
    - iii. identification requirements/procedures; and
    - iv. notifying officers’ names, agency, and telephone numbers.
  - d. Notifying officers should conduct a follow-up within 24 hours with any survivor when there is concern for the survivor’s well-being.
- O. Driving Under the Influence by a Minor
- 1. When a minor (a person who is under the age of 21) is operating a motor vehicle in a public place and has introduced alcohol into their body but is not intoxicated, officers determine if there is any detectable amount of alcohol in the minors system. The smell of alcohol on the minor’s breath constitutes detectable amount. DUI is not a lesser included offense to DWI.
  - 2. The officer shall conduct Standardized Field Sobriety Tests (SFST), including the use of a portable breath testing device, if possible, and document the results in their offense reports.
  - 3. If an arrest for DWI is not made and the officer determines the minor has a detectable amount of alcohol in their system, the officer may:
    - a. Issue a citation and complete a DIC-25, DIC-23, and release the minor to a responsible adult.
    - b. If there is no responsible adult available, the subject is taken into custody and booked into jail on the appropriate charges.

- c. If an arrest is made for DWI and a specimen of breath (Intoxilyzer Test) or blood is requested, then all standard DWI procedures are followed.
4. Disposition of Evidence
- a. When an officer arrests or issues a citation to a person for any other alcohol-related Class C misdemeanor or city ordinance violation, he/she will seize any alcoholic beverage in the possession of the person at the time of the arrest or citation
  - b. Alcoholic beverage containers seized in accordance with the preceding paragraph will be disposed of as follows:
    - i. If the person arrested or cited is under 21 years of age, each container, whether opened or unopened, will be poured out and the container properly discarded, after attaining photographs of the evidence being disposed.
    - ii. Destruction of any alcoholic beverage at the scene is done within view of the officer's patrol units video camera or body camera.

#### P. Criminal Trespass

1. Criminal Trespass is a misdemeanor that requires notice for removal from property or that entry is forbidden, and commission does not constitute a breach of the peace. Therefore, an arrest without a warrant must be for an on-view offense.
2. Enforcement Action
  - a. Upon contacting the suspect, the officer shall obtain identification and check for warrants. The officer shall determine if a Criminal Trespass Warning has been issued to the suspect by interviewing the complainant and/or checking CopSync.
  - b. If a warning has not been issued, the officer will complete a Trespass Warning in CopSync and give a copy to the suspect, with instruction that if they return, they will be arrested.
  - c. A copy of the warning will also be given to the property owner or representative of the owner.
3. If a warrantless arrest is made, it is necessary that an officer be present whenever a suspect is verbally notified to depart from the premises.
4. It is legally permissible for a second officer to make a warrantless arrest for criminal trespass if the suspect has been issued a trespass warning by another officer. Information about who issued the warning is included in the case report.
5. If the suspect has never been given a prior trespass warning, an officer cannot make a warrantless jail arrest for criminal trespass when the suspect is being held against his will by a security guard, business owner, etc. Follow the above steps if proved that the subject had received a criminal trespass warning.
6. Disregarding signs, fences and locked or unlocked habitations is evidence that the subject received warning and can be arrested without the pursuit of a warrant.

#### Q. Drug Paraphernalia

1. All drug paraphernalia seized in connection with a drug arrest will be placed in the property room and properly booked in as evidence with the following exceptions:
  - a. When the seizure and arrest is for an amount of marijuana less than a usable amount or is for paraphernalia only, with no other drug charge, the following process will be used.
    - i. The officer will check the subject for wanted and if clear, issue a citation for Possession of Drug Paraphernalia. The Paraphernalia charge will be the first charge on the citation if more than one charge is cited.
    - ii. The Paraphernalia and or drug residue will be seized and placed in a bag for transport to the police facility.
    - iii. Upon arrival at the police facility, the seizing officer will, in the presence of a second officer, photograph the evidence, and then destroy and dispose of the paraphernalia.
  - b. A copy of the photograph will be submitted, with the citation and offense report, to the Municipal Court. The seizing officer will indicate the manner of the destruction of the paraphernalia in their offense report and the witnessing officer will provide a supplemental report regarding the destruction.

#### R. Escorts

1. Personnel shall refrain from providing non-emergency escorts unless requested by another Law Enforcement Agency, a City, County or State agency. Such escorts are limited to:
  - a. Funerals.
  - b. Hazardous materials.
  - c. Oversize vehicles, only when necessary to provide expeditious travel though the city to avoid unnecessary traffic delays.
  - d. Dignitaries and public officials
2. Medical Escorts:
  - a. Officers shall refrain from providing emergency medical escorts to private vehicles, except when such escort is of such short distance that medical attention would clearly be delayed by utilization of ambulance personnel.
  - b. In the case of minor injury, the officer may direct the parties to the nearest medical facility or location for assistance. For those more seriously injured, an ambulance should be requested to the scene.
  - c. Extreme caution should be utilized during such escorts.

#### S. Family Disturbances/Family Violence

1. Officers investigate family violence cases and are strongly encouraged to make appropriate arrests of family violence suspects, to end the possibility of further violence being committed on the victim. Officers will refer to Policy 7.13 for

operational procedures. If an arrest is not able to be made, articulate why not in the offense report.

2. If the victim of family violence does not want to prosecute the suspect, officers shall still make the arrest. Officers will refrain from telling the complainant that charges can be dropped later.
3. If the suspect is not at the scene, officers will make diligent efforts to apprehend the suspect, if the suspect is believed to be in proximity to the scene and it is believed the suspect may return and engage in further family violence.
4. Officers will collect and preserve evidence in family violence situations in the same manner that such evidence is collected and preserved in other criminal cases.
5. Officers shall give all victims or alleged victims of family violence a Family Violence Victim Notice, which may be printed from our CopSync System.
6. Officers should consult with the victim to determine if an Emergency Protective Order (EPO) is needed.
7. Required Reporting Documentation
  - a. Case Report (if family violence occurred)
  - b. Family Violence Report (if family violence occurred)
  - c. Assault Victims' Statement (if family violence occurred)
  - d. Magistrate's Information Sheet
  - e. Green Sheet for County Jail Officials.

#### T. Fireworks

1. Officers should act when these violations are observed or brought to their attention. Patrol officer may file charges against adults for displaying, possessing, shooting, throwing fireworks etc. under City Ordinances.
2. If the offender is a juvenile, the officer will contact the juvenile's parents or guardian, inform them of the violation, and file the appropriate charges.
3. All confiscated fireworks are destroyed on video camera. Under no circumstances shall fireworks (explosives) be placed in the departmental evidence system.

#### U. Hazardous Materials (TBP: 8.12)

1. In the event of a case involving hazardous materials, the officer shall contact the Teague Volunteer Fire Department immediately and take the appropriate action to protect life and property. This may include evacuating or limiting access to the scene. The Teague Volunteer Fire Department personnel will undertake the command and control of hazardous material scenes and hold responsibility for all removal and cleanup measures that are undertaken.
2. The Teague Volunteer Fire Department has the equipment and training, or contact information for those that do, required to properly respond to Hazardous Materials



and Bio-Hazard incidents, including Protective Equipment as well as decontamination equipment.

#### V. Injured Persons

1. Patrol officers are dispatched to respond to injured person calls (other than those resulting from criminal activity, motor vehicle accidents, cases of major magnitude, or if the injury occurs on city property) only when the presence of the officer will protect life, render first aid, or restore order.
2. In the event a child or elderly person has been injured a case report may be generated if the officer believes negligence was involved.
3. For this section, a child is a person under 15 years of age and an elderly person is over 64 years of age.
4. If the person is injured on city property, a case report is always generated and forwarded to the Chief of Police for notification of appropriate city personnel.

#### W. Junk and Abandoned Vehicles

1. Texas Laws and a City Ordinance authorize the Police Department to take into custody an abandoned motor vehicle found on public or private property.
2. Texas Laws and City Ordinance allow authorized persons to enter private property to examine vehicles or vehicle parts, obtain information as to the identity of the vehicle, and cause the removal of a vehicle or vehicle part that constitutes a nuisance when so ordered by the judge of the municipal court or Board of Aldermen.
3. Procedures for removal of abandoned or junk vehicle-public property  
Vehicles found left unattended creating a hazardous traffic situation require immediate removal out of the roadway.
4. Officers shall determine if the vehicle meets the criteria to be classified as an abandoned motor vehicle. A Violation Warning Sticker is affixed to the vehicle in the following manner:
  - a. Place sticker on the rear window either on the lower left or right side - whichever can easily be seen by passing motorists.
  - b. Do not place sticker in a position in which it may obstruct the driver's view.
  - c. Do not place on any painted surface.
  - d. Do not place more than one sticker on any vehicle.
  - e. If the vehicle is towed the officer shall write a report and have the vehicle entered in TCIC/NCIC as stored/abandoned.
5. Procedures for removal of abandoned or junk vehicles - private property
  - a. The police department is responsible for removal of vehicles on private property in accordance with applicable laws and city ordinances.

#### X. Juvenile Parties and Large Gatherings

1. Officers responding to calls regarding juvenile parties and gatherings will investigate each call to determine if a criminal offense has taken place. Officers are to conduct their investigations following State Law and Departmental Policy to determine the correct course of action.
2. If the violation of law involves a Class C Misdemeanor officers are not authorized to enter a residence or fenced in area of the residence, without first obtaining consent to enter from an individual who holds possessory interest in the property, regardless if the violation is an on view offense. All other entry into any residence or fenced property should be supported by:
  - a. probable cause to believe that a criminal offense classified as a Class B Misdemeanor or higher is in progress, and
  - b. urgent circumstances exist where an officer would not have time to secure a search warrant, or
  - c. consent from someone with possessory interest in the property, or
  - d. a reasonable belief that immediate entry is necessary to protect anyone from physical harm.
3. If it is determined an offense has taken place, officers are to take appropriate enforcement action following established guidelines.
4. If a violation has been determined to involve a minor, the parents or guardian of the minor will be contacted and requested to come to the scene to take custody of the violator, after signing a Receipt for Child Form.
5. Evidence obtained will be photographed and disposed of following established guidelines.

#### Y. Liquor Law Violations

1. When an arrest is made in licensed premises because intoxicated persons are permitted to remain on the premise [T.A.B.C Section 104. (6)] a copy of the arrest reports is to be provided to the Texas Alcoholic Beverage Commission.
2. In order that desired administrative action be taken, the arrest report must contain the following additional information if applicable:
  - a. Observation by the arresting officer that the licensee or his employee is permitting the intoxicated person to remain on the premise. (or was in the position to see the intoxicated person but did nothing to cause him to be removed).
  - b. Identity of the licensee or the employee who served the intoxicated person (name, age, physical description, address, and employment status).
  - c. Res Gestae statements made by the licensee, employee, or intoxicated person.
  - d. Answers to questions made by the licensee, employee/ and/or intoxicated person.
  - e. The TABC license number for the premises (obtained from their permit that should be publicly visible).

## Z. Major Crime Scenes

1. Initial responding officers shall initiate the preliminary investigation and perform tasks as designated below until otherwise directed by a superior officer, or other officer specifically assigned to criminal investigations.
2. In transit to crime scenes, officers shall be cognizant of suspects/vehicles that may be in flight.
3. Upon arrival the officer should:
  - a. Verify that a crime has been committed and relay essential information to communications.
  - b. Summon emergency medical assistance if required and take those steps necessary to protect victims or others.
  - c. Arrest/detain the perpetrator if at the scene. A decision to leave the crime scene to arrest or pursue the perpetrator should be made based on weighing the immediate needs of victims and others against the safety of the public, if the perpetrator were allowed to escape.
  - d. Provide communications with such information as:
    - i. nature of the crime committed.
    - ii. description of the perpetrator and mode/direction of flight.
    - iii. description of any vehicle used by the offender and any accomplices.
    - iv. use of firearms or other deadly weapons; and
    - v. any support required at the crime scene.
  - e. Identify any witnesses to the crime, secure their identities and request that they remain present at the crime scene until they can be interviewed.
  - f. Where reasonably possible, obtain the identities on any other persons who were present upon arrival at the crime scene
  - g. Note the license tags of vehicles parked near the crime scene and be aware of suspicious persons on hand at or near the crime scene.
  - h. Provide superior officers and any other investigative personnel arriving on the scene with complete information on the offense and the measures taken thus far by officers and others.
  - i. Responding officers shall enter crime scenes only for purposes of aiding victims or bystanders in need of immediate assistance, apprehending perpetrators or securing the area.
  - j. Officers making initial entries for the above purposes shall, where feasible, avoid touching, walking upon, moving objects, or otherwise altering or contaminating the crime scene. Officers shall advise supervisory personnel of exit and entry paths.
  - k. Define the boundaries of the crime scene to include all areas that may reasonably be searched for evidence. As necessary, considering the nature and seriousness of the crime, officers should:
    - i. request backup assistance to restrict access to the crime scene and control any on-lookers.

- ii. erect barricade tape, rope or cordon off, lock, or otherwise secure the immediate crime scene and restrict access to defined crime perimeters; and
  - iii. record any alterations made at the crime scene due to emergency assistance to victims, the actions of persons reporting the crime, handling of any items of evidentiary value or other actions.
  - iv. document anyone entering the crime scene on a crime scene log.
- l. Restrict all persons from the crime scene who are not directly involved in the investigation. In the case of homicides or other major crimes the officer-in-charge (OIC) shall ensure that the identity of all persons entering the crime scene is recorded on the crime scene log.
  - m. Homicides and other major crime scenes should be approached only as needed in a single defined line to avoid destruction of footprints and other impressions and the contamination of scent trails that may be useful in canine searches. The “place last seen” of kidnapped or missing persons should also be protected in a similar manner.

AA. Missing Persons / Kidnapping / Attempted Child Abductions

1. Reporting/Classification of Missing Persons

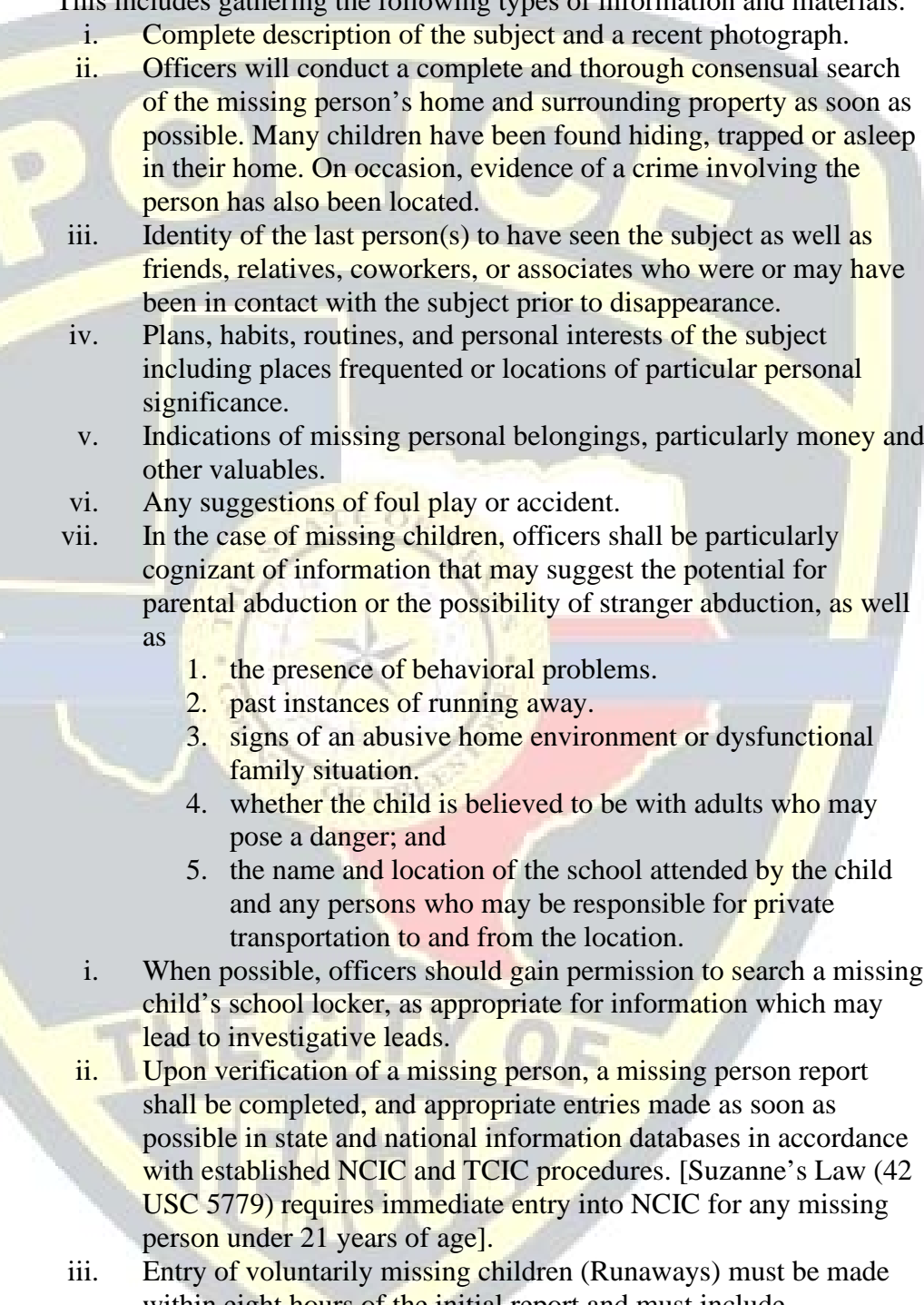
- a. Officers receiving a report of a possible kidnapping or child abduction will immediately cause notification of a supervisor and the Chief of Police. In cases of a potential kidnapping or child abduction, time is of the essence and the department may initiate preplanned protocols for handling these events.
- b. Reports of unsuccessful attempted child abductions will require a field unit response and offense report as well as immediate TLETS notification of the Texas Clearinghouse.
- c. There is no waiting period for reporting a missing person. Missing person reports shall be taken in-person or by telephone in conformance with the criteria of this policy and the criticality of the incident.
- d. A person may be declared “missing” when his/her whereabouts is unknown and unexplainable for a period of time that is regarded by knowledgeable parties as highly unusual or suspicious in consideration of the subject’s behavior patterns, plans or routines.
- e. An individual may be considered “missing-critical” who meets the foregoing criteria and among other possible circumstances:
  - i. A reasonable suspicion the individual may be the subject of foul play.
  - ii. Under 13 or over 65 and may be unable to properly safeguard or care for himself/herself.
  - iii. suffers from diminished mental capacity or medical conditions that are potentially life threatening if left untreated/unattended.

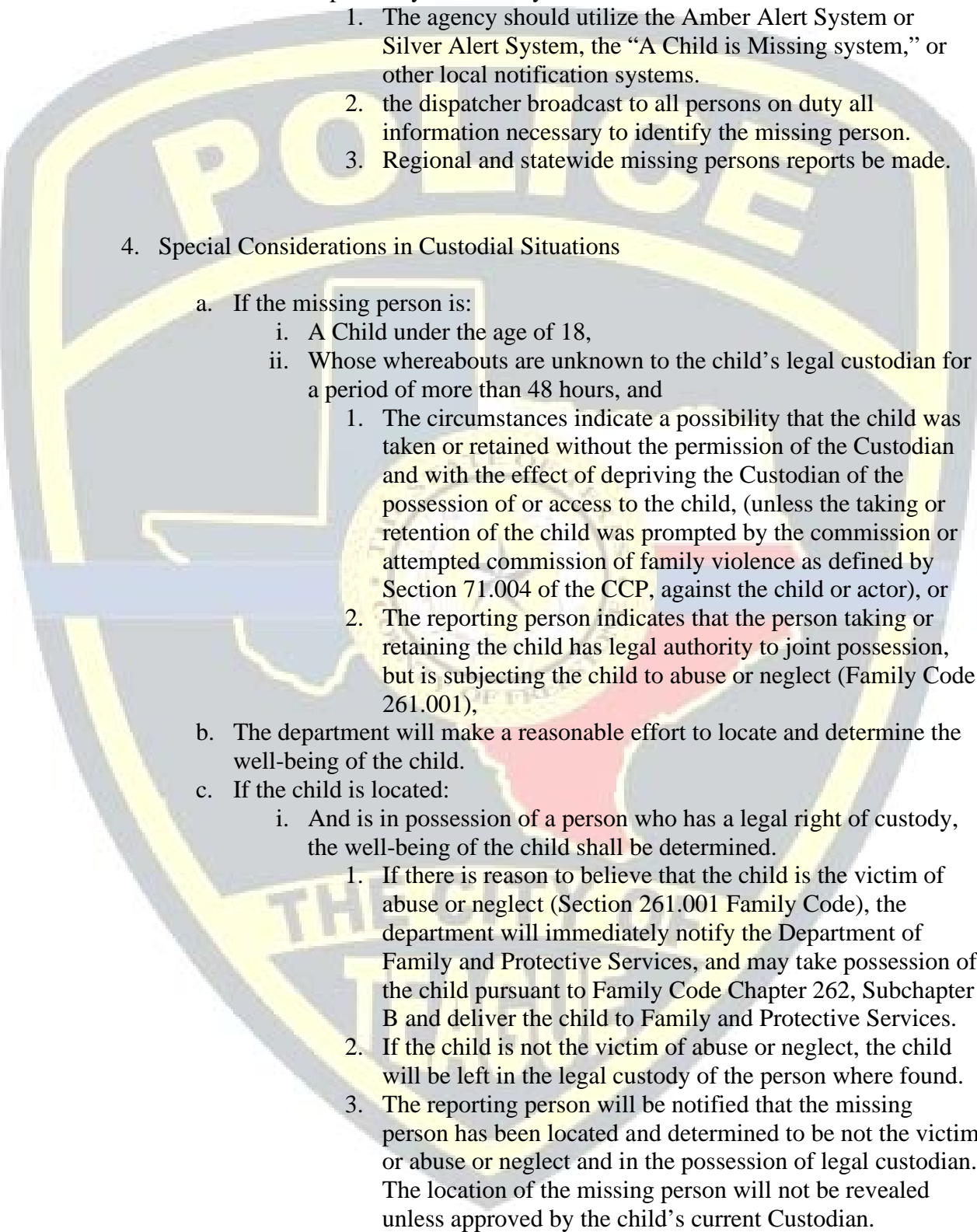
- iv. is a patient of a mental institution and is considered potentially dangerous to himself or others.
- v. has demonstrated the potential for suicide; or
- vi. may have been involved in a boating, swimming or other sporting accident or natural disaster.
- f. On any Critical Missing, the department will continue active investigation by assigning personnel full time in attempting to locate the missing person.
- g. Reports of juveniles who have voluntarily left home (i.e., “runaways”) should be classified as such only after thorough investigation. The number of incidents where a child has left home voluntarily should be determined and whether the child is in a natural or foster home. This information is needed for data entry into NCIC and TCIC.

## 2. Initial Report Taking

- a. The responding officer must gather as much pertinent information as quickly as possible to properly classify a missing person report and initiate proper response. This includes the following information:
  - i. Name, age and physical description of the subject and relationship of the reporting party to the missing person.
  - ii. Time and place of last known location and the identity of anyone accompanying the subject.
  - iii. The extent of any search for the subject.
  - iv. Whether the subject has been missing on prior occasions and the degree to which the absence departs from established behavior patterns, habits, or plans.
  - v. Whether the individual has been involved recently in domestic incidents; suffered emotional trauma or life crises; demonstrated unusual, uncharacteristic, or bizarre behavior; is dependent on drugs or alcohol or has a history of mental illness.
    - i. The current physical condition of the subject and whether the person is currently on prescription medication.
- b. If the missing person is a child, inquiry should also determine if the child
  - i. is or may be with any adult who could cause him/her harm.
  - ii. may have been the subject of a parental abduction.
  - iii. has previously run away from home, has threatened to do so, or has a history of explainable or unexplainable absences for extended periods of time.
  - iv. The current custodial status of the child.
- c. A supervisory officer shall be contacted on all missing persons cases.

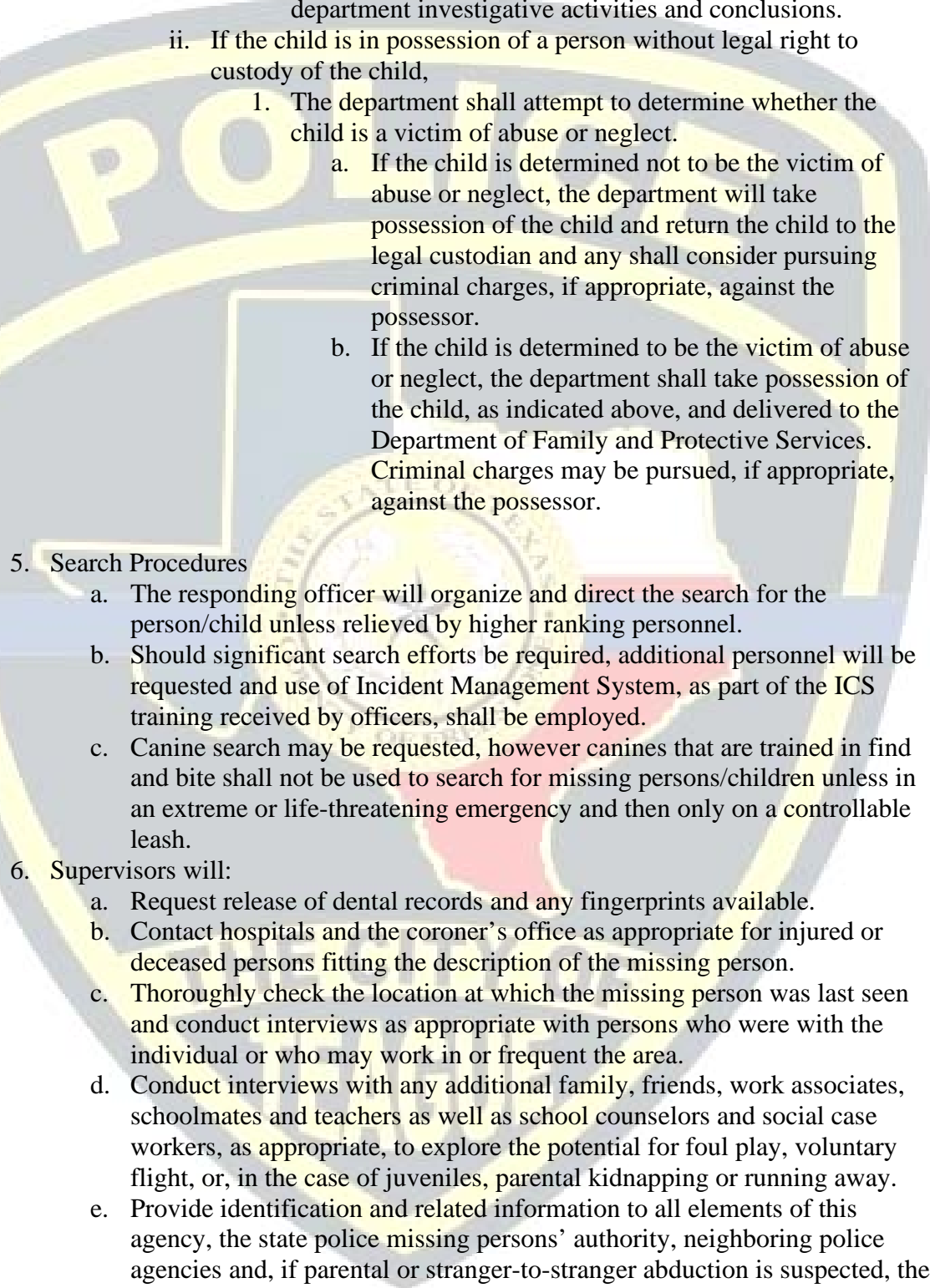
## 3. Preliminary Investigation

- 
- a. The preliminary investigation is intended to gather information and to take those steps that will aid in the search for and location of a missing person. This includes gathering the following types of information and materials:
- i. Complete description of the subject and a recent photograph.
  - ii. Officers will conduct a complete and thorough consensual search of the missing person's home and surrounding property as soon as possible. Many children have been found hiding, trapped or asleep in their home. On occasion, evidence of a crime involving the person has also been located.
  - iii. Identity of the last person(s) to have seen the subject as well as friends, relatives, coworkers, or associates who were or may have been in contact with the subject prior to disappearance.
  - iv. Plans, habits, routines, and personal interests of the subject including places frequented or locations of particular personal significance.
  - v. Indications of missing personal belongings, particularly money and other valuables.
  - vi. Any suggestions of foul play or accident.
  - vii. In the case of missing children, officers shall be particularly cognizant of information that may suggest the potential for parental abduction or the possibility of stranger abduction, as well as
    1. the presence of behavioral problems.
    2. past instances of running away.
    3. signs of an abusive home environment or dysfunctional family situation.
    4. whether the child is believed to be with adults who may pose a danger; and
    5. the name and location of the school attended by the child and any persons who may be responsible for private transportation to and from the location.
- i. When possible, officers should gain permission to search a missing child's school locker, as appropriate for information which may lead to investigative leads.
  - ii. Upon verification of a missing person, a missing person report shall be completed, and appropriate entries made as soon as possible in state and national information databases in accordance with established NCIC and TCIC procedures. [Suzanne's Law (42 USC 5779) requires immediate entry into NCIC for any missing person under 21 years of age].
  - iii. Entry of voluntarily missing children (Runaways) must be made within eight hours of the initial report and must include information as required by DPS rules regarding their entry.
  - iv. Reports of Attempted Child Abductions will be made to the Texas Clearing House using TLETS as required by DPS rules as soon as possible.

- 
- v. In the case of persons designated as “missing- critical,” a supervisory officer may direct that
    - 1. The agency should utilize the Amber Alert System or Silver Alert System, the “A Child is Missing system,” or other local notification systems.
    - 2. the dispatcher broadcast to all persons on duty all information necessary to identify the missing person.
    - 3. Regional and statewide missing persons reports be made.

#### 4. Special Considerations in Custodial Situations

- a. If the missing person is:
  - i. A Child under the age of 18,
  - ii. Whose whereabouts are unknown to the child’s legal custodian for a period of more than 48 hours, and
    - 1. The circumstances indicate a possibility that the child was taken or retained without the permission of the Custodian and with the effect of depriving the Custodian of the possession of or access to the child, (unless the taking or retention of the child was prompted by the commission or attempted commission of family violence as defined by Section 71.004 of the CCP, against the child or actor), or
    - 2. The reporting person indicates that the person taking or retaining the child has legal authority to joint possession, but is subjecting the child to abuse or neglect (Family Code 261.001),
- b. The department will make a reasonable effort to locate and determine the well-being of the child.
- c. If the child is located:
  - i. And is in possession of a person who has a legal right of custody, the well-being of the child shall be determined.
    - 1. If there is reason to believe that the child is the victim of abuse or neglect (Section 261.001 Family Code), the department will immediately notify the Department of Family and Protective Services, and may take possession of the child pursuant to Family Code Chapter 262, Subchapter B and deliver the child to Family and Protective Services.
    - 2. If the child is not the victim of abuse or neglect, the child will be left in the legal custody of the person where found.
    - 3. The reporting person will be notified that the missing person has been located and determined to be not the victim or abuse or neglect and in the possession of legal custodian. The location of the missing person will not be revealed unless approved by the child’s current Custodian.

- 
4. A Missing Person offense report will be made and a supplement to the offense will be made outlining all department investigative activities and conclusions.
    - ii. If the child is in possession of a person without legal right to custody of the child,
      1. The department shall attempt to determine whether the child is a victim of abuse or neglect.
        - a. If the child is determined not to be the victim of abuse or neglect, the department will take possession of the child and return the child to the legal custodian and any shall consider pursuing criminal charges, if appropriate, against the possessor.
        - b. If the child is determined to be the victim of abuse or neglect, the department shall take possession of the child, as indicated above, and delivered to the Department of Family and Protective Services. Criminal charges may be pursued, if appropriate, against the possessor.
  5. Search Procedures
    - a. The responding officer will organize and direct the search for the person/child unless relieved by higher ranking personnel.
    - b. Should significant search efforts be required, additional personnel will be requested and use of Incident Management System, as part of the ICS training received by officers, shall be employed.
    - c. Canine search may be requested, however canines that are trained in find and bite shall not be used to search for missing persons/children unless in an extreme or life-threatening emergency and then only on a controllable leash.
  6. Supervisors will:
    - a. Request release of dental records and any fingerprints available.
    - b. Contact hospitals and the coroner's office as appropriate for injured or deceased persons fitting the description of the missing person.
    - c. Thoroughly check the location at which the missing person was last seen and conduct interviews as appropriate with persons who were with the individual or who may work in or frequent the area.
    - d. Conduct interviews with any additional family, friends, work associates, schoolmates and teachers as well as school counselors and social case workers, as appropriate, to explore the potential for foul play, voluntary flight, or, in the case of juveniles, parental kidnapping or running away.
    - e. Provide identification and related information to all elements of this agency, the state police missing persons' authority, neighboring police agencies and, if parental or stranger-to-stranger abduction is suspected, the FBI.



- f. Decisions to use local media to help locate missing persons shall be made with the approval of the Chief of Police and the missing person's family.
- g. The Primary Case Investigator shall maintain routine on-going contact with the missing person's closest relative concerning progress of the investigation. These and other relevant individuals shall be informed that they must notify the primary case investigator as soon as any contact is made with the missing person.

7. Recovery of Missing Persons and Case Closure

- a. Competent adults, having left home for personal reasons, cannot be forced to return home. Officers locating such individuals shall:
  - i. advise them that they are the subject of a wanted to locate investigation.
  - ii. ask if they desire the reporting party or next-of-kin to be notified of their whereabouts; and
  - iii. make provisions to transmit this information to the reporting party or next-of-kin if permitted by the missing person.
- b. In all cases, reporting parties shall be informed of the well-being of located missing persons. Unless criminal matters necessitate other action, desires of missing persons not to reveal their whereabouts shall be honored.
- c. Missing persons shall be questioned to establish the circumstances surrounding their disappearance and whether criminal activity was involved.
- d. In cases involving juveniles, officers shall ensure that:
  - i. the juvenile receives medical attention in a timely manner, if necessary.
  - ii. initial questioning of the youth identifies the circumstances surrounding the child's disappearance, any individuals who may be criminally responsible and/ or whether an abusive or negligent home environment was a contributory factor, and
  - iii. that parents, guardians and/or the person reporting the missing youth are notified in a timely manner.
- e. Upon location of a missing person, all agencies and information systems previously contacted for assistance will be notified or updated.

BB. Parking Violations

- 1. Officers actively enforce parking ordinances in:
  - a. handicapped spaces.
  - b. fire lanes; and
  - c. no parking zones.
- 2. Special attention is given to parking violations in the following circumstances:
  - a. high traffic areas.
  - b. peak traffic times; and
  - c. high complaint areas

3. Enforcement activity is only undertaken in areas lawfully designated by official means or as stipulated by State law.
4. Officers may remove vehicles in an emergency situation or with the approval of a Supervisor in a non-emergency situation, and in accordance with established law.

CC. Protective Orders

1. A Protective Order is issued by a court that finds that family violence has occurred and is likely to occur again.
2. Protective orders are usually valid for a period of one year. Officers must ascertain that the Protective Order is valid before taking any enforcement action.
3. Officers dispatched to an address should be informed by Communications if a Protective Order is in effect at the address at which they are responding to. Communications should also inform the officers of the identity of those listed in the order.
4. If, through the officer's investigation, it is determined a violation of a protective order has occurred, the violator shall be arrested.
5. Once the order has been in effect, no party involved, including the victim, can allow a violation to take place.

DD. Robbery Investigations

1. Crime Scene Control
  - a. The initial responding patrol officer secures the crime scene and ensures the protection of evidence from victims, suspects, witnesses, spectators, and other law enforcement personnel. Adequate perimeters will be established for the preservation of the crime scene. Officers shall remove or cause to be removed any animals or other conditions which may adversely affect the integrity of the scene. Officers shall request additional assistance as needed.
  - b. Personnel may enter the crime scene only if they have a legitimate law enforcement function to perform there, and only at the discretion of the Crime Scene Investigator. They are always accompanied by a Crime Scene Investigator.
2. Supervisor Response
  - a. The responding supervisor assumes direct control of the scene.
  - b. The supervisor shall direct any assistance that is required and designate an officer to secure the crime scene if the initial officer must assume other duties, i.e., take custody of offender, accompany victim to hospital, etc.
  - c. A supervisor shall assign an officer the task of maintaining a crime scene log containing the names of individuals entering and exiting the crime scene including the time of entry/exit.
  - d. A supervisor shall assign officers to conduct a neighborhood inquiry:
  - e. Persons near the scene will be interviewed concerning what they may have seen or heard as well as what they know about the victim and his/her associates

## EE. Robbery in Progress Calls for Service

1. On all robbery in progress calls a minimum of two (2) officers should be dispatched to the scene.
2. Upon Arrival the Following Takes Place:
  - a. The officers shall establish an exterior perimeter.
  - b. Officers shall not enter the building until they are certain there are no robbers inside.
  - c. When the perimeter is set, they will request communications contact the business.
  - d. Communications will instruct the business representative, to come outside and meet with the officers.
  - e. Upon speaking with the business representative communications will notify the officers as to the following:
    - i. Name of the subject coming out.
    - ii. Description, including clothing.
    - iii. The identification of the subject will be verified by officers.
3. Unless circumstances prevent, in the event the suspects are still inside the business, officers should refrain from contacting any suspect until they exit the building.

## FF. Sexual Assault Investigations

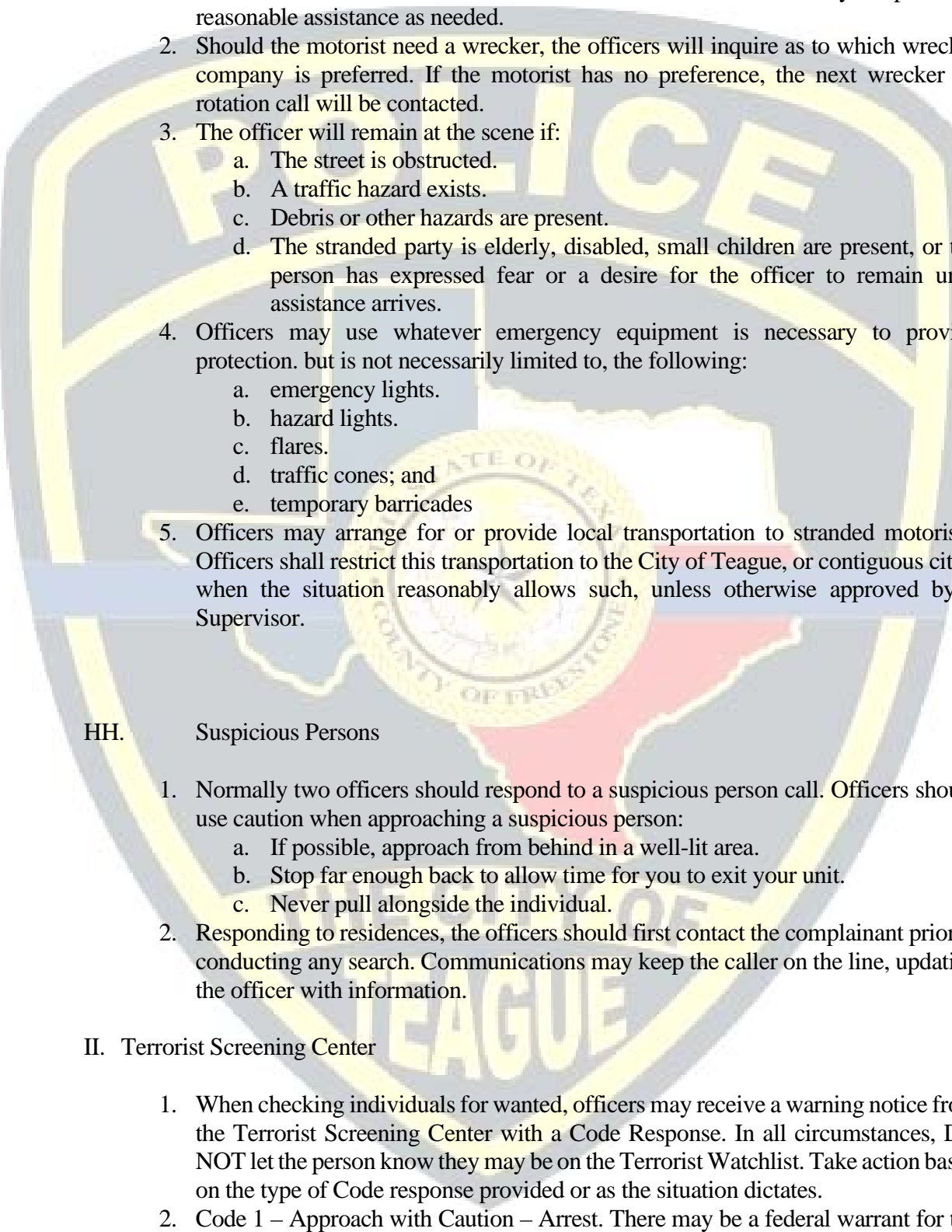
1. Initial Officer Response
  - a. As part of the emergency response, officers shall:
    - i. Contact the victim as soon as possible to address safety concerns and summon emergency medical assistance if needed.
    - ii. Attempt to obtain a suspect description immediately and broadcast to other officers
    - iii. Evaluate the scene for people, vehicles, or objects involved as well as possible threats
    - iv. Relay all vital information to responding officers and supervisors, including any possible language barriers
    - v. Secure the crime scene to ensure that evidence is not lost, changed, or contaminated
    - vi. Request response from supervisors as appropriate
    - vii. Begin a search for the suspect when appropriate
2. Assisting the Victim
  - a. As part of the emergency response, officers shall:
    - i. Show understanding, patience, and respect for the victim's dignity and attempt to establish trust and rapport.
    - ii. Inform the victim that an officer of the same sex will be provided if desired and available.
    - iii. Contact a victim advocate as soon as possible to provide assistance throughout the reporting and investigative process.

- iv. Supply victims of sexual assault with the phone number for the Rape, Abuse, and Incest National Network (RAINN) Hotline, 1-800-656-HOPE. Operators at this hotline connect the caller with the rape crisis center closest to the victim's location.
- b. Request a response from supervisors, and clearly explain his or her role and limit the preliminary interview so that the victim is not then asked the same questions by a supervisor.
- c. Be aware that a victim of sexual assault may bond with the first responding officer. It is important to explain the role of the different members of the sexual assault response team and help with transitions through introductions.
- d. Record observations of the crime scene, including the demeanor of the suspect and victim and document any injuries or disheveled clothing.

### 3. Evidence Collection Issues

- a. Officers shall introduce the need for a medical examination to the victim explaining the importance of investigative and apprehension efforts as well as for the victim's well being.
- b. If field officers are required to collect or assist in collecting evidence, proper evidence collection procedures will be used.
- c. DNA evidence plays a crucial role in the sexual assault investigation. In addition to the victim's and suspect's bodies and clothing, there are many other potential sources such as condoms, sheets, blankets, pillows, and bottles that may contain biological evidence such as blood, sweat, tissue, saliva, hair, and urine. To properly collect DNA evidence, officers shall:
  - i. Use sterile gloves and change as needed.
  - ii. Use sterile swabs, papers, solutions, and tools.
  - iii. Package evidence in individual envelopes.
  - iv. Avoid touching the area where potential DNA evidence may exist.
  - v. Avoid talking, sneezing, and coughing over evidence.
  - vi. Air dry evidence before packaging.
  - vii. Put evidence into new paper bags or envelopes, not plastic.
- d. The sexual assault evidence kit shall be accepted from the medical staff after it has been properly sealed and labeled.
- e. The kit will contain whole blood that requires that the kit be placed and logged into an evidence refrigerator or delivered directly to the Texas Department of Public Safety Crime Lab as soon as possible. The kit may also contain a urine sample for toxicology testing. If it does, the urine sample shall also be refrigerated or delivered directly to the Texas Department of Public Safety Crime Lab as soon as possible.
- f. The kit shall not be allowed to freeze or be exposed to heat such as being near a car's interior heater.

GG. Stranded Motorists

- 
1. Motorists who are stranded due to accident or mechanical difficulty are provided reasonable assistance as needed.
  2. Should the motorist need a wrecker, the officers will inquire as to which wrecker company is preferred. If the motorist has no preference, the next wrecker on rotation call will be contacted.
  3. The officer will remain at the scene if:
    - a. The street is obstructed.
    - b. A traffic hazard exists.
    - c. Debris or other hazards are present.
    - d. The stranded party is elderly, disabled, small children are present, or the person has expressed fear or a desire for the officer to remain until assistance arrives.
  4. Officers may use whatever emergency equipment is necessary to provide protection, but is not necessarily limited to, the following:
    - a. emergency lights.
    - b. hazard lights.
    - c. flares.
    - d. traffic cones; and
    - e. temporary barricades
  5. Officers may arrange for or provide local transportation to stranded motorists. Officers shall restrict this transportation to the City of Teague, or contiguous cities when the situation reasonably allows such, unless otherwise approved by a Supervisor.

#### HH. Suspicious Persons

1. Normally two officers should respond to a suspicious person call. Officers should use caution when approaching a suspicious person:
  - a. If possible, approach from behind in a well-lit area.
  - b. Stop far enough back to allow time for you to exit your unit.
  - c. Never pull alongside the individual.
2. Responding to residences, the officers should first contact the complainant prior to conducting any search. Communications may keep the caller on the line, updating the officer with information.

#### II. Terrorist Screening Center

1. When checking individuals for wanted, officers may receive a warning notice from the Terrorist Screening Center with a Code Response. In all circumstances, DO NOT let the person know they may be on the Terrorist Watchlist. Take action based on the type of Code response provided or as the situation dictates.
2. Code 1 – Approach with Caution – Arrest. There may be a federal warrant for the subject, take necessary precautions and arrest if a warrant exists.

3. Code 2 – Approach with Caution – Detain. There may be a federal detainer notice for the subject. Take necessary safety precautions and detain while contacting the Terrorist Screening Center.
4. Code 3 – Approach with Caution. Arrest only if there is evidence of a local, state, or federal crime. Do not let the subject know they may be on the Terrorist Watchlist. Gather as much information as possible regarding suspect’s identity, associates, and current addresses. Contact the Terrorist Screening Center with the information as soon as possible.
5. The Terrorist Screening Center can be contacted at 866-872-9001

## **VI. EQUIPMENT MAINTENANCE AND READINESS**

### **A. Vehicle Maintenance Procedure**

1. Employees assigned a department vehicle assume responsibility to ensure that any malfunctions or mechanical problems with the assigned vehicle are promptly reported through the established reporting procedures.
2. The dealer performs all warranty maintenance of department vehicles while under warranty.
3. A private vendor may be utilized for out of warranty vehicles.
4. All such maintenance is scheduled through work orders forwarded to the fleet maintenance sergeant.
5. Any employee experiencing difficulties with any vehicle of this department during their tour of duty that would obviously cause additional damage to the unit shall:
  - a. Discontinue its use; and
  - b. Complete vehicle inspection form.
6. All requests for maintenance work on department vehicles are documented on a vehicle inspection form.
7. No employee shall alter, or authorize the alteration, of any vehicle, without the approval of the Chief of Police.

### **B. Equipment Maintenance Procedure**

1. Maintenance and servicing of all department equipment is scheduled through the Administrative Assistant.
2. Any employee experiencing a malfunction or failure of any equipment belonging to the Department shall report the problem via email, including their immediate supervisor in the email.
3. All requests for maintenance work to be done on department equipment will be documented.
4. Each employee of this department is responsible to ensure that any equipment issued by the department is kept in good repair and working order.
5. Personal equipment obtained at the expense of the employee is maintained and repaired at the employee's expense.
6. Maintenance of Inventory:

- a. Officers shall conduct a pre-shift inspection of their assigned patrol unit, noting any deficiencies on their Vehicle Inspection form.
- b. Supplies should be replenished immediately when depleted.

#### C. Equipment Readiness

1. All equipment assigned to the patrol division is kept in a state of readiness. Patrol Supervisors are responsible for the maintenance and readiness of all equipment assigned to the Police Department

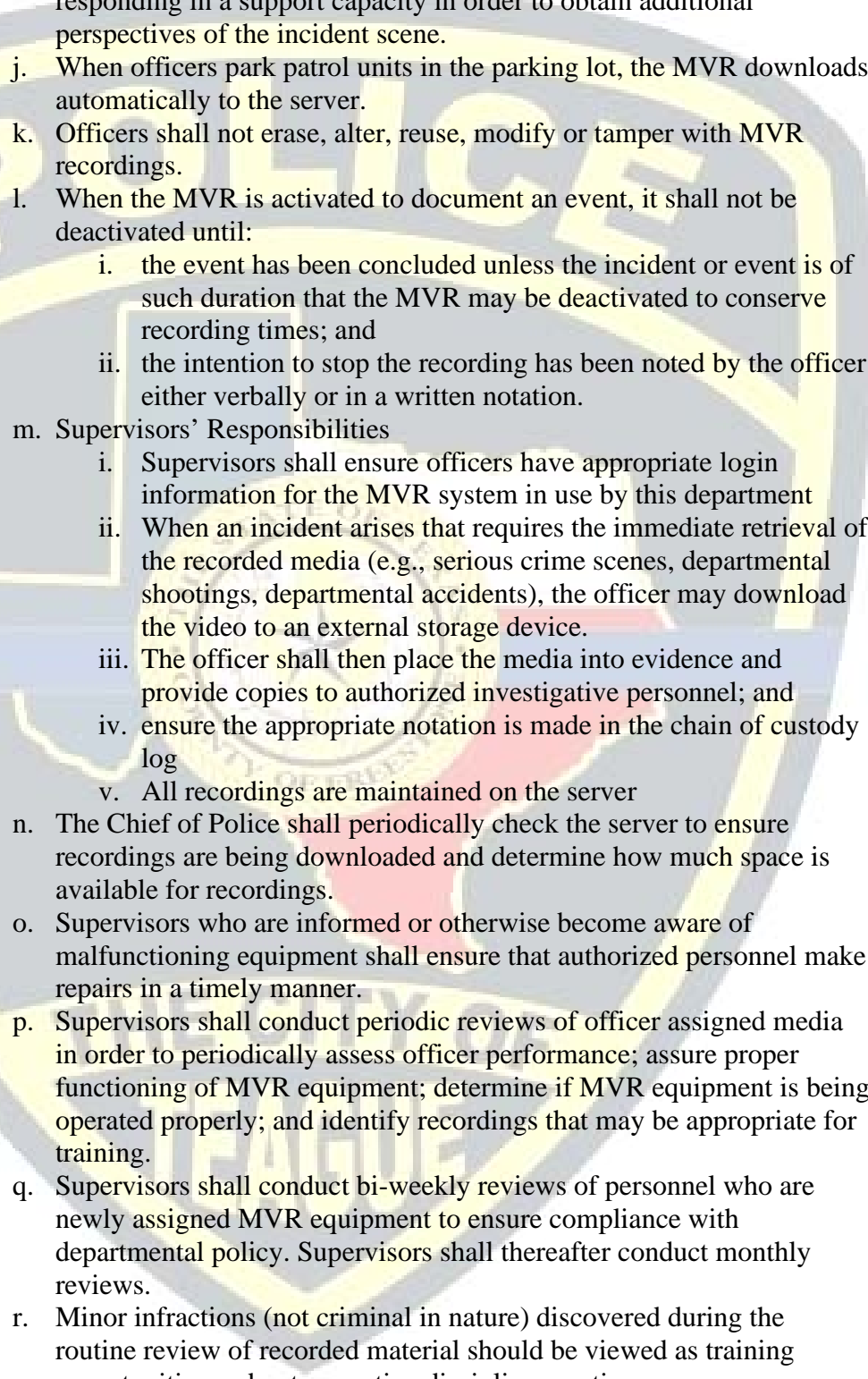
#### D. Knife Use and Safety

1. This department recognizes the need for its officers to be properly equipped to handle a wide variety of duty responsibilities. Officers may carry folding utility knives as authorized by this policy and consistent with their duty assignment.
2. The knife is intended solely for the purpose of carrying out the general duties and designated specialized assignments of police operations; its use as a defensive or offensive weapon is authorized only in exigent circumstances when deadly force is authorized.
3. Knives shall be folded and secured by a fastening device so as to ensure officer safety, knife retention, and concealment. The blade and securing device shall be carried in the least obtrusive manner possible, whether the officer is on or off duty, and consistent with the officer's duty assignment or tactical deployment.
4. Folding blade knives shall conform to agency-defined quality standards to meet the demands of work assignments as defined by this standard operating procedure and the officer's supervising officer. The cutting edge of such knives shall not exceed four and one-half inches in length as measured from blade tip to handle. Authorized users shall not:
  - a. Display a knife in any offensive or threatening manner without legitimate operational justification.
  - b. Carry a knife in any manner other than clipped in a pocket or waistband, or inside the pants or vest.
  - c. Carry a knife while handling prisoners in a custodial facility, except when needed for rescue, suicide prevention, or other authorized purposes as determined by supervisory officers.
5. Uses as a Weapon. The knife is not intended for use as a weapon and officers are discouraged from using it in this capacity. However, if it is used in defensive or offensive capacities under exigent circumstances, it shall be deemed a use of deadly force and is governed by this department's policies on use of force to include, but not be limited to, summoning a supervisor and reporting it as a use of force.

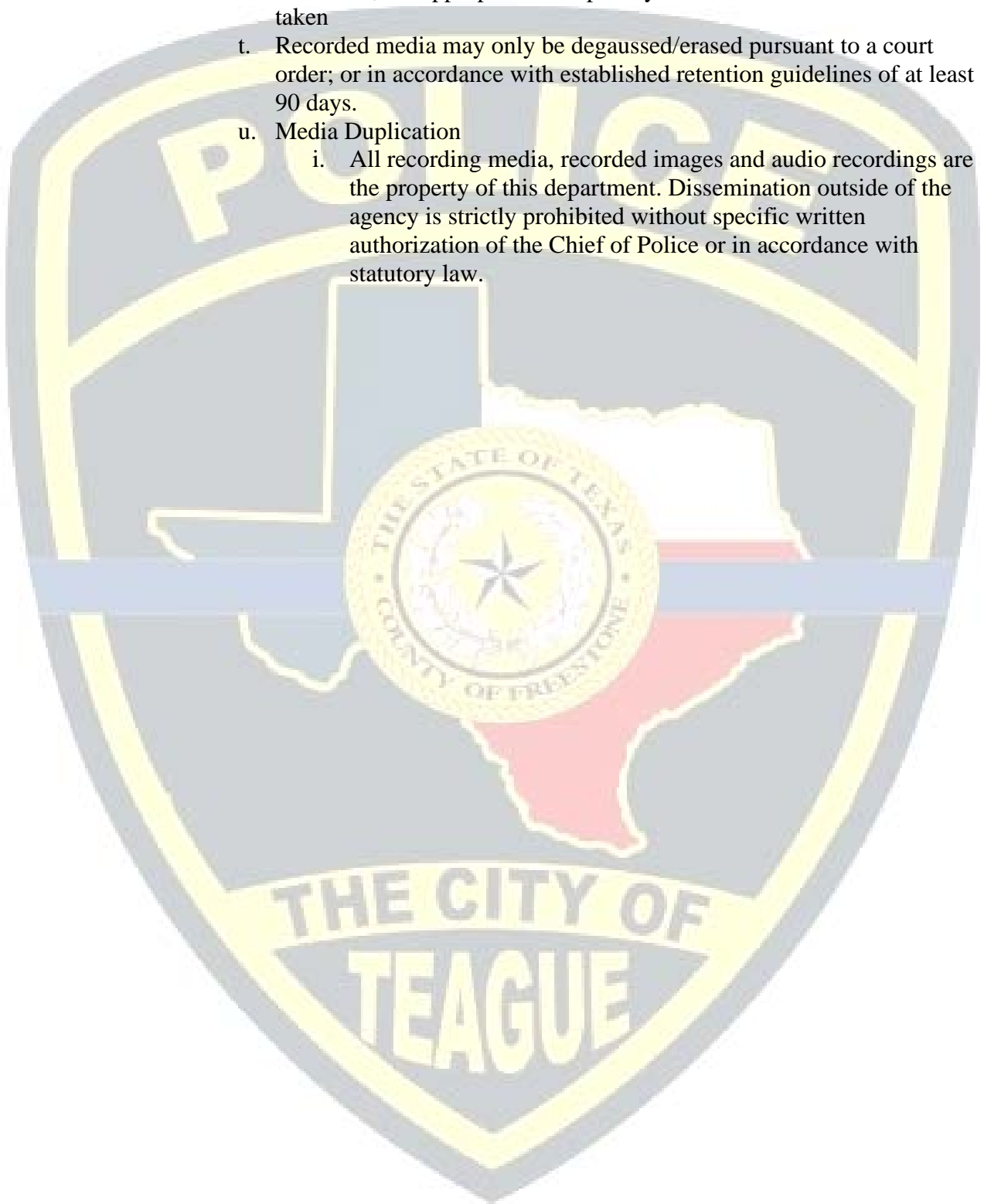
#### E. Mobile Video Recording System

1. The use of a Mobile Video Recording (MVR) system provides persuasive documentary evidence and helps defend against civil litigation and allegations of officer misconduct.
2. Officers assigned the use of these devices shall adhere to the operational objectives and protocols outlined herein to maximize the effectiveness and utility of the MVR and the integrity of evidence and related video documentation.
3. General Procedures
  - a. It shall be the responsibility of this department to ensure that the audio-video recording equipment is properly installed according to the manufacturer's recommendations. MVR equipment shall automatically activate when emergency equipment (lights) or a wireless transmitter is operating. The system may also be activated manually from the control panel affixed to the interior of the vehicle.
  - b. Placement and operation of system components within the vehicle shall be based on officer safety requirements.
  - c. All officers shall successfully complete this department's approved course of instruction prior to being deployed with MVR systems in operational settings.
  - d. Inspection and general maintenance of MVR equipment installed in departmental vehicles shall be the responsibility of the officer assigned to the vehicle.
  - e. Prior to beginning each shift, the assigned officer shall perform an inspection to ensure that the MVR is performing in accordance with the manufacturer's recommendations covering the following matters.
    - i. Remote activation of system via transmitter
    - ii. Windshield and camera lens free of debris
    - iii. Camera facing intended direction
    - iv. Recording mechanism capturing both audio and video information - System plays back both audio and video tracks.
    - v. Log into the system to personalize the recording
  - f. Malfunctions, damage or theft of in-car camera equipment shall be reported to the immediate supervisor prior to placing the unit into service.
  - g. Mandatory Use:
    - i. All official contacts whether on a call or officer initiated.
    - ii. Traffic stops (to include, but not limited to traffic violations, stranded motorist assistance and all crime interdiction stops)
    - iii. Priority responses
    - iv. Vehicle pursuits
    - v. Prisoner transports
  - h. When the MVR is activated, officers shall ensure that the audio portion is also activated so all events are properly documented. Officers are encouraged to narrate events using the audio recording, to provide the best documentation for pretrial and courtroom presentation.



- 
- i. Officers using transmitters that are individually synchronized to their individual MVR shall activate both audio and video recordings when responding in a support capacity in order to obtain additional perspectives of the incident scene.
  - j. When officers park patrol units in the parking lot, the MVR downloads automatically to the server.
  - k. Officers shall not erase, alter, reuse, modify or tamper with MVR recordings.
  - l. When the MVR is activated to document an event, it shall not be deactivated until:
    - i. the event has been concluded unless the incident or event is of such duration that the MVR may be deactivated to conserve recording times; and
    - ii. the intention to stop the recording has been noted by the officer either verbally or in a written notation.
  - m. Supervisors' Responsibilities
    - i. Supervisors shall ensure officers have appropriate login information for the MVR system in use by this department
    - ii. When an incident arises that requires the immediate retrieval of the recorded media (e.g., serious crime scenes, departmental shootings, departmental accidents), the officer may download the video to an external storage device.
    - iii. The officer shall then place the media into evidence and provide copies to authorized investigative personnel; and
    - iv. ensure the appropriate notation is made in the chain of custody log
    - v. All recordings are maintained on the server
  - n. The Chief of Police shall periodically check the server to ensure recordings are being downloaded and determine how much space is available for recordings.
  - o. Supervisors who are informed or otherwise become aware of malfunctioning equipment shall ensure that authorized personnel make repairs in a timely manner.
  - p. Supervisors shall conduct periodic reviews of officer assigned media in order to periodically assess officer performance; assure proper functioning of MVR equipment; determine if MVR equipment is being operated properly; and identify recordings that may be appropriate for training.
  - q. Supervisors shall conduct bi-weekly reviews of personnel who are newly assigned MVR equipment to ensure compliance with departmental policy. Supervisors shall thereafter conduct monthly reviews.
  - r. Minor infractions (not criminal in nature) discovered during the routine review of recorded material should be viewed as training opportunities and not as routine disciplinary actions.

- s. Should the behavior or action become habitual after being informally addressed, the appropriate disciplinary or corrective action shall be taken
- t. Recorded media may only be degaussed/erased pursuant to a court order; or in accordance with established retention guidelines of at least 90 days.
- u. Media Duplication
  - i. All recording media, recorded images and audio recordings are the property of this department. Dissemination outside of the agency is strictly prohibited without specific written authorization of the Chief of Police or in accordance with statutory law.



***TEAGUE***  
***POLICE DEPARTMENT***



**Performance Evaluation Manual**

## **GENERAL INSTRUCTIONS:**

Performance evaluation is an important process for both supervisors and employees. It is a tool that can enhance the operation of the department, and it is also a process that allows employees to be both recognized for good performance and provided with recommendations for improvement. Remember that if your employee succeeds, then you as a supervisor succeed. **While performance evaluation is not simple, it nevertheless remains a primary responsibility of those functioning in a supervisory role.**

All employees must have their performance evaluated in writing at least once a year, on the anniversary of their hire date.

**Special Note for Supervisors of Probationary Employees:** The probationary period allows the supervisor the opportunity to judge whether an employee is carrying out the duties in his/her job description. For an employee to succeed, he or she must be provided with appropriate supervision, and adequate feedback. The performance evaluation form you will complete for the probationary employee is the same as the form used for non-probationary employees. On the cover sheet however, you will need to identify whether the review is an end of training, six months, nine months, or final review. You will also be asked to recommend, or not recommend that the employee be continued in his/her appointment at the end of each review, or that an employee be reappointed as a permanent employee at the completion of his/her probationary period.

The Sworn Officer Evaluation Form must be completed by the immediate supervisor. Because a supervisor can forget instance that occurred during an early part of a rating cycle, it is imperative that supervisors maintain a notebook where the supervisor makes performance notes regarding officer activity daily. This notebook as well as the officer's personnel file should be reviewed prior to completing the performance evaluation.

Part I of the Evaluation Form requires the supervisor to rate the officer on the various job-related functions of the job. The supervisor should refer closely to the rating guide that is part of this manual to properly rate whether the officer is Superior, Acceptable, or Unacceptable. Any rating of less than 3 must be accompanied by specific comments that justify the rating. The comments that justify any rating of 3 or less will be placed on a separate sheet of paper entitled "Documentation" and should include details of how this was communicated to the employee and what actions were recommended to overcome the deficiency.

In Part II, supervisors must complete the performance narrative. This section requires the supervisor to specifically identify positive performance and provide the officer with positive reinforcement for the outstanding work accomplished during the year.

This section also requires the supervisor to identify any weaknesses the officer may have and to recommend actions for improvement.

In Part III, the supervisor and officer should agree on at least three performance goals for the upcoming evaluation period. Employee input on both goals and performance evaluations are important.

Remember that during the evaluation interview the communication should be two-way: the supervisor should use the opportunity to convey his/her assessment of the staff member's work, and encourage the staff member to comment on his/her own work. Following the discussion, supervisors may adjust the written evaluation if necessary. Also remember to give the employee a copy of the evaluation for his/her records.

### **PITFALLS IN MAKING PERFORMANCE APPRAISALS**

- A. **The Isolated Incident**  
No rating should be based on a few isolated performance incidents. When this is done, the rating is unfairly influenced by non-typical instances of favorable or unfavorable performances.
- B. **The "Halo" Effect**  
The "Halo" effect occurs when one factor influences ratings on all factors. Examples: An employee's work is of good quality, therefore, other ratings (such as those on promptness or work quantity) are higher than normal. Another employee is frequently absent, with the result that the ratings on other factors are usually low.
- C. **The "Cluster" Tendency**  
The tendency to consider everyone in the work group as above average, average, or below average. Some raters are considered "tough" because they normally "cluster" their people at a low level. Others are too lenient. "Clustering" overall ratings usually indicates that the rater has not sufficiently discriminated between high and low levels of performance.
- D. **Rating the Job and Not the Individual**  
Individuals in more difficult jobs are often considered superior performers to those in lower-rated jobs. This normally means that confusion exists between the performance appraisal and how the job has been evaluated.
- E. **Length of Service Bias**  
There is a tendency to allow the period of an individual's employment to influence the rating. Normally, performance levels should be higher as an individual gains training and experience, but this is not always the case.
- F. **Personality Conflicts**  
Avoid judgments made purely based on personality traits. Effective, efficient employees do not necessarily agree with everything a supervisor believes in or states.

## **SUGGESTIONS FOR ACCURAT EVALUATIONS**

- A. Consider the entire appraisal period. Try to enumerate high points and low points in performance, then assign a rating that typifies the individual's normal performance. Do not attempt to assign a rating to a performance indicator and then create justification to support it. Be able to explain the reason for each rating.
- B. Rate each indicator independently. When evaluating more than one person simultaneously, it may be helpful to rate all employees' performances on one indicator rather than one employee's performance on all factors. Use the summary evaluation to give substance to individual factors.
- C. In a group of people in similar jobs, performance is likely to be spread over most performance categories. Review your own record as a rater. Check the tendency to be either "too tough" or "too lenient" in your appraisals.
- D. Consider how an individual is performing in relation to what is expected. Rate the person's performance, not importance of the job.
- E. Recognize that some people may never achieve top ratings, regardless of length of service. Watch closely the progress of newcomers and be ready to recognize superior performance if it is achieved.

It is incumbent upon each employee, regardless of level or category, to perform in an exemplary manner reflecting those principles and disciplines upon which this department was founded. Used constructively, this program of performance evaluation can prove to be a valuable tool regarding individual career advancement, and result in increased productivity throughout all areas of the department.

## **RATING SCALE VALUES**

The task of evaluating and rating an officer's performance shall be based on the following numerical scale value definitions. These definitions serve as a means of standardizing the evaluation process.

### **(1) DRIVING SKILLS: STRESS CONDITIONS**

1. Unacceptable: Involved in accident(s). Overuses red/blue lights and siren. Excessive and unnecessary speed. Fails to slow for intersections or loses control on corners.
3. Acceptable: Maintains control of vehicle. Evaluates driving situations and reacts properly. Proper speed for conditions.
5. Superior: High degree of reflex ability and competence in driving skills. Superior judgment shown in use of lights and siren. Controls speed skillfully.

(2) DRIVING SKILLS: NON-STRESS CONDITIONS

1. Unacceptable: Continually violates traffic law (red/blue lights, speed, stop signs, etc.). Involved in chargeable accidents. Lacks dexterity and coordination during vehicle operation.
3. Acceptable: Able to maintain control of vehicle while being alert to activity outside vehicle. Practices good defensive driving techniques.
5. Superior: Sets good examples of lawful, courteous driving while exhibiting good manipulative skill in operating the radio, using the street index, etc.

(3) ORIENTATION SKILL

1. Unacceptable: Becomes disoriented when responding to stressful situations. Unable to relate his/her location to their destination. Unable to use map under stress. Unable to determine compass directions during stressful situations.
3. Acceptable: Aware of his/her location. Able to use map effectively under stress. Demonstrates good sense of direction when responding to stressful situations.
5. Superior: Always responds quickly to stressful calls by the most appropriate route. Does not have to refer to map. Does not become disoriented during stressful situations. Calmly operates the radio and coordinates the responses of other officers.

(4) FIELD PERFORMANCE: STRESS CONDITIONS

1. Unacceptable: Becomes emotional and panic stricken. Unable to function; loses temper. Endangers safety of self and other officers and citizens by inattention to the demands of the job.
3. Acceptable: Exhibits a calm and controlled attitude. Can perform reasonably well at least in preventing a situation from deteriorating. Reasonably conscious of officer safety measures and protection of citizens from further harm.
5. Superior: Maintains control and brings order under virtually any circumstances without assistance. Remembers and carries out key police duties properly.

(5) FIELD PERFORMANCE: NON-STRESS CONDITIONS

1. Unacceptable: Confused and disoriented as to what action should be taken in each situation. Numerous specific examples of bad judgment can be shown.

3. Acceptable: Able to assess situation and take proper action.
5. Superior: Requires no assistance and always takes proper action. Excellent field judgment.

(6) OFFICER SAFETY: GENERAL

1. Unacceptable: Frequently fails to exercise basic officer safety precautions. Examples:
  - a. Exposes weapons (baton, handgun, etc) to suspect.
  - b. Fails to keep gun hand free during enforcement situations.
  - c. Stands directly in front of violator's car door.
  - d. Fails to control suspect's movements.
  - e. Does not maintain sight of violator while writing summons.
  - f. Fails to use illumination when necessary.
  - g. Fails to advise radio when leaving vehicle.
  - h. Fails to maintain good physical condition.
  - i. Fails to use or maintain personal safety equipment properly.
  - j. Does not foresee potentially dangerous situations.
  - k. Points weapon at other officers.
  - l. Stands too close to vehicular traffic.
  - m. Stands in front of door when knocking.
  - n. Fails to have weapon ready when appropriate.
  - o. Fails to cover other officers.
  - p. Fails to search police vehicle before duty or after transporting prisoners.
  - q. Fails to check equipment.
  - r. Fails to properly search or handcuff prisoners.
3. Acceptable: Understands principles of officer safety and generally applies them.
5. Superior: Always maintains position of safety and advantage. Does not become unduly anxious or apprehensive, over-cautious or overconfident.

(7) OFFICER SAFETY: WITH SUSPICIOUS PERSONS AND PRISONERS

1. Unacceptable: Frequently violates officer safety standards. Fails to "pat search" or confronts suspicious persons while seated in patrol vehicle. Fails to handcuff prisoners. Fails to thoroughly search prisoners or vehicles. Fails to maintain a position of advantage with prisoners.
3. Acceptable: Generally, displays awareness of potential danger from suspicious persons and prisoners. Maintains position of advantage.



5. Superior: Always maintains position of advantage and is alert to changing conditions.

(8) CONTROL OF CONFLICT: VOICE COMMAND

1. Unacceptable: Improper voice inflection, i.e., too soft, too loud, indecisive, confused commands, etc. Few problems resolved as result of officer's oral direction.
3. Acceptable: Speaks with authority in a calm, clear voice.
5. Superior: Always appears to be in complete command through voice tone and bearing.

(9) CONTROL OF CONFLICT: PHYSICAL SKILL

1. Unacceptable: Cowardly, physically unable to handle most situations, or uses too much or too little force for given situations.
3. Acceptable: Maintains control without excessive force. Maintains self in good physical condition.
5. Superior: Excellent knowledge of and ability to use restraining holds. Always ready to use necessary force. Maintains above average physical condition.

(10) INVESTIGATIVE PROCEDURES

1. Unacceptable: Does not plan an investigative strategy. Cannot define investigative goals, i.e., successful prosecution, arrest, recovery of property, development of informants. Leaves out important steps in investigations. Fails to connect legal and departmental guidelines while conducting investigation. Cannot coordinate aspects of the investigation, i.e., interviews, searches, notetaking, report-writing.
3. Acceptable: Maintains command of a crime scene. Able to assess the requirements of the situation concerning collection and preservation of evidence, interviews, and interrogations. Undertakes most of these functions with little or no direction.
5. Superior: Requires no supervision in organizing and undertaking an investigation. Identifies all possible sources of physical evidence. Identifies all potential witnesses and victims. Conducts complete interview. Uses time efficiently.

(11) REPORT WRITING: ORGANIZATION AND DETAILS

1. Unacceptable: Incapable of organizing events into written form. Leaves out many important details. Puts in inappropriate information. Much of the work will have to be redone.
3. Acceptable: Converts field events into a logical sequence of thought to include all elements of the situation. The narrative leaves the reader with a good understanding of what took place.
5. Superior: A complete and detailed account of what occurred from beginning to end. Written and organized so that any reader has a clear understanding of what occurred. Full consideration is given to the needs of investigator/prosecutor.

(12) PROPER FORM SELECTION: ACCURACY AND DETAILS

1. Unacceptable: Unable to determine proper forms for given situations. Forms filled out incorrectly or incompletely.
3. Acceptable: Knows most standard forms and understands format. Completes forms with reasonable accuracy.
5. Superior: Consistently and rapidly completes detailed forms with no assistance. High degree of accuracy.

(13) REPORT WRITING: GRAMMAR/SPELLING/NEATNESS

1. Unacceptable: Illegible, misspelled words, incomplete sentence structure.
3. Acceptable: Grammar, spelling, and neatness are satisfactory in that errors are rare and do not impair understanding.
5. Superior: Very neat and legible. No spelling mistakes and excellent grammar.

(14) REPORT WRITING: APPROPRIATE TIME USED

1. Unacceptable: Requires 2-3 hours to correctly complete a basic simple report.
3. Acceptable: Correctly completes simple basic reports in thirty minutes.
5. Superior: Correctly completes simple basic reports in no more time than that of a skilled veteran officer. (Depending on the type of report, the time will vary.)

(15) RADIO: LISTENS AND COMPREHENDS TRANSMISSIONS

1. Unacceptable: Repeatedly misses call sign and is unaware of radio traffic in adjoining beats. Frequently must ask dispatcher to repeat transmissions or does not understand message.
3. Acceptable: Copies most radio transmissions directed at him/her. Generally aware of adjoining beat radio traffic.
5. Superior: Always comprehends radio transmissions and makes a written record. Always aware of and reacts to radio traffic in adjoining beats.

(16) RADIO: ARTICULATION OF TRANSMISSIONS

1. Unacceptable: Does not plan before transmitting message. Under or over modulation, resulting in dispatcher or other units constantly asking for a repeat.
3. Acceptable: Uses proper procedure with short, clear, concise transmissions.
5. Superior: Always uses proper procedure with clear, calm voice, even under stress conditions.

(17) SELF-INITIATED ACTIVITY

1. Unacceptable: Does not see or avoids activity. Does not follow up on situations; rationalizes suspicious circumstances. Gets involved inappropriately too often. Ignores departmentally defined problems.
3. Acceptable: Recognizes and identifies suspected criminal activity. Makes cases from routine activity. Makes recommendations for directed patrol. Promotes departmental crime-prevention programs. Networks with private and public associations or agencies.
5. Superior: Catalogs, maintains, and uses information given at briefings and from bulletins or crime reports for reasonable cause to stop persons or vehicles. Makes quality arrests. Shows balance in the type and extent of self-initiated activity. Combines directed patrol with community involvement through development of mutual respect and trust. Consistently develops and shares intelligence with other team officers. Actively develops and nurtures Neighborhood Watch programs.

(18) PROBLEM SOLVING/DECISION-MAKING ABILITY

1. Unacceptable: Acts without thought or is indecisive. Relies on others to make decisions. Numerous examples of bad decisions or indecision can be shown.

3. Acceptable: Able to reason out problems and relate them to what he/she was taught. Has good perception and ability to make own decisions. Maintains minimal informal community contacts consistent with departmental community-oriented policing objectives.
5. Superior: Excellent perception in foreseeing problems and arriving at advanced decisions. Makes timely, quality decisions. Recommends or submits proposals concerning community partnerships to attack specific crime problems. Adept at mediating, negotiating, solving community problems informally. Acts as liaison to relevant non-profit agencies such as food banks and the Girl and Boy Scouts. Consistently alert to ways of improving the quality of life in the officer's assigned community.

(19) COMMUNITY-POLICING OBJECTIVES

1. Unacceptable: Maintains a minimal reactive policing profile in the community. Not proactive in developing informal community contacts or developing Neighborhood Watch alliances with citizens. Minimal promotion of crime-prevention techniques.
3. Acceptable: Organizes Neighborhood Watch alliances with citizens; distributes crime-prevention literature and promotes crime-prevention methods and philosophy when interacting with citizens; gives referrals to social-assistance agencies. Visits local businesses to enlist help in crime prevention.
5. Superior: Not only offers citizen referrals to social-assistance agencies, but actively seeks and executes opportunities to link social services agencies to citizens, obtain code enforcement, and coordinate drug treatment, improved sanitation or animal control, or noise abatement. Actively advises landlords, contractors, and others about CPTED (crime prevention through environmental design). Organizes and coordinates the work of volunteers.

(20) KNOWLEDGE OF DEPARTMENTAL ORDERS

1. Unacceptable: Has little knowledge of departmental orders. Makes no attempt to learn them. Frequent violations of orders.
3. Acceptable: Familiar with commonly applied rules and procedures; can apply them to most field situations.
5. Superior: Exceptional working knowledge of rules, procedures, and orders.

(21) KNOWLEDGE OF CRIMINAL LAW

1. Unacceptable: Does not know the elements of basic offenses. Reports and performance continually show inability to apply criminal law to field situations.
3. Acceptable: Has a working knowledge of commonly used sections of code. Relates elements to observed criminal behavior.
5. Superior: Outstanding knowledge of criminal law. Able to apply laws to normal and unusual criminal activity.

(22) KNOWLEDGE OF TRAFFIC LAW

1. Unacceptable: Does not know the elements of basic offenses. Reports or actions continually show inability to apply traffic law to field situations.
3. Acceptable: Has a working knowledge of commonly used sections of code. Relates elements to observed traffic activity.
5. Superior: Outstanding knowledge of traffic law. Able to apply laws to normal and unusual traffic related activity.

(23) ACCEPTANCE OF FEEDBACK: VERBAL/BEHAVIOR

1. Unacceptable: Argumentative, rationalizes, refuses to admit mistakes, refuses to make corrections. Always considers feedback negative.
3. Acceptable: Accepts criticism in a positive manner and applies it to further learning. Accepts responsibility for his or her mistakes.
5. Superior: Solicits feedback and criticism to improve performance. Never argues with or blames others.

(24) RELATIONSHIPS WITH CITIZENS

1. Unacceptable: Abrupt, belligerent, overbearing, officious, introverted, or uncommunicative.
3. Acceptable: Courteous, friendly, and empathetic. Communicates in a professional and unbiased manner.
5. Superior: Establishes rapport and is always fair.

(25) RELATIONSHIPS WITH SUPERVISORS, CO-WORKERS

1. Unacceptable: Constantly argues with other officers or other superior officers. Belittles other officers or supervisors in front of other people. Fails to adhere to chain of command. Insubordinate.
3. Acceptable: Able to establish a good relationship with other officers and supervisors. Understands and adheres to chain of command. Respects other officers.
5. Superior: Establishes excellent relationships with other officers and supervisors. Possesses thorough understanding of chain of command and adheres to it. Utmost respect shown to superior officers and peers as well.

(26) GENERAL Demeanor

1. Unacceptable: Officer cannot be depended upon to produce routine work without close supervision. Does not adapt readily to new situations, work hours, changing assignments. Tardy, complains about assignments, days off, duties.
3. Acceptable: Officer generally displays initiative, interest in the job, willingness to take on new challenges or schedule changes. Dependable.
5. Superior: Attentive beyond requirements of job. Constantly analyzes own work performance and devises and tries new approaches to problems. Consistently outstanding overall performance. High interest in welfare and image of department. Exemplary.

(27) GENERAL APPEARANCE

1. Unacceptable: Overweight, dirty shoes, uniforms, and leather. Long messy hair. Offensive body odor.
3. Acceptable: Neat, clean, and well-pressed uniform. Cleaned and shined shoes and leather. Well-groomed hair.
5. Superior: Tailored uniforms, spit-shined shoes, and leather. Command bearing.



---

# Report Writing Manual

---

Teague Police Department

---

May 2021

---

TEAGUE POLICE DEPARTMENT  
REPORT WRITING MANUAL

PART I  
GENERAL REPORT WRITING GUIDELINES



## **PURPOSE**

The purpose of this manual is to provide guidance to police officers of the Teague Police Department regarding report writing. A law enforcement officer's ability to document the facts and activities of an incident directly reflects of the professionalism of the officer and the department and affects the ability of the justice system to successfully prosecute a criminal case.

## **INTRODUCTION**

Nearly half of a police officer's work involves writing, and because of this, the best arrests will go unprosecuted if the reporting officers do not have the necessary writing skills to record their actions in a case clearly, concisely, and accurately, with sufficient detail.

An officer's report must document every incident in a complete, clear, and concise manner. Any arrest, follow up investigation, prosecution, or administrative action that is to be taken because the report must be initiated, supported, or justified by the information contained solely within the body of the report.

Consequently, every police report must be able to withstand critical review and legal scrutiny, and must be truthful, unbiased, and unprejudiced. Moreover, police officers have a moral and legal obligation to investigate all crimes that are reported to them and provide documentation of their findings in the form of a report.

## **USES OF POLICE REPORTS**

Police reports have many different uses, both within the criminal justice system and beyond:

### **Identification of Criminals**

Police reports assist with the identification, apprehension, and prosecution of criminals by serving as a source document for filing criminal complaints, by providing a record of all calls for service, investigations/observations, and providing a basis for additional follow up investigations.

### **Investigative Record**

Police reports aid prosecutors, defense attorneys, and other law enforcement agencies by providing records of investigations and serving as source documents for criminal prosecution, as well as documenting agency actions.

### **Court Preparation**

Police reports assist officers prior to or during court appearances by refreshing the officer's memory before testifying or preparing to provide hearsay testimony at preliminary hearings.

### **Civil Liability Assessment**

Police reports are essential for risk managers, insurance companies, and civil litigation attorneys for use in determining potential civil liability by documenting events such as accidents or injuries on city property, workman's compensation type injuries, as well as to presenting justification for an officer's behavior or actions in a citizen complaint, officer complaint, or lawsuit against the officer/city.

## **Statistical Analysis**

Police reports assist police and administrators as well as the community by providing statistical information for analysis of crime trends, equipment needs, manpower issues, continued professional training requirements, and assist in the evaluation of officer performance.

## **CHARACTERISTICS OF AN EFFECTIVE POLICE REPORT**

Everyday police officers are faced with a variety of events and incidents. Officers, at each of these, are required to make significant decisions, oftentimes without delay, and while under stress or the benefit of all the facts regarding the situation. For this reason, crime and incident reports must reflect the details of the specific crime or incident for further reference and use. While the details of every incident or crime report will likely vary, there are six characteristics that all effective reports have in common.

An effective police report is always:

1. **Factual.** A police report is an objective accounting of the relevant and observed facts of the case, and any conclusions made by the reporting officer must be supported by articulable facts. An effective report never includes unsubstantiated opinions or conclusions.
2. **Accurate.** The decisions and actions taken must be supported by accurate information contained in the report. If any information is inaccurate, the credibility and reliability of the report and officer will likely be jeopardized. Accuracy is achieved by carefully, precisely, and honestly reporting of all relevant information.
3. **Clear.** A police report speaks for the reporting officer when he or she is not present. There should be no doubt or confusion regarding what happened during an incident or crime, based upon the content of a police report. Clarity in report writing is achieved by clear and logical organization of information, the judicious use of simple, common, and first-person language, and effective writing mechanics.
4. **Concise.** Reports should be brief but also contain all relevant information necessary for a complete understanding of the crime or incident, without additional explanation. Brevity should never take precedence over accuracy, completeness, or clarity in report writing.
5. **Complete.** A complete report will contain all the relevant facts, information, and details that the reader will need to have for a comprehensive understanding of the crime or incident described in the report. The report is comprehensive when it is a complete word picture of the incident, there are no questions left unanswered by the reader, officer actions are explained and justified by the contents of the report, and both supporting and conflicting information is included.
6. **Timely.** No decisions can be made, or actions taken, regarding an arrest or request for follow up investigation if a report is not submitted in a timely fashion.

## **FIELD NOTES**

An officer's field notes are the original source documents used to write a police report. For this reason, if field notes are incomplete, poorly organized, or illegible, they will be of little use to the officer in writing the resulting police report. For this reason, field notes should always be taken at the scene, especially when interviewing a suspect, victims, or witnesses and whenever the officer wishes to remember specific details later.

When writing field notes, officers should consider that field notes are typically more reliable than memory, especially since reports are typically written several hours after a specific incident or crime has occurred. This time lapse can often cause an officer to easily forget or confuse certain types of information, especially times, observations, addresses, and key words and phrases from statements. Moreover, the prudent use of field notes can minimize or even eliminate the need to recontact the involved parties in a case later.

Every event, incident, and crime are different from one another, and for this reason, the facts and information needed by the officer to write a police report is different. However, field notes and reports should always be able to answer the questions what, where, when, who, how, and why regarding the incident.

Regardless of how the individual officer decides to take field notes, the following information is a snapshot of the items that should be included in field notes.

	<b>Basic Information</b>	<b>Additional Information</b>
<b>Victims and Witnesses</b>	<ul style="list-style-type: none"> <li>• Full name</li> <li>• Age</li> <li>• Date of birth</li> <li>• Race</li> <li>• Sex</li> <li>• Telephone numbers (home, work, cellular)</li> <li>• Address</li> <li>• Email address(es)</li> </ul>	<ul style="list-style-type: none"> <li>• How to contact by telephone or in person</li> <li>• Best place to contact</li> <li>• Best time to contact</li> <li>• Place of employment (including name and telephone number)</li> </ul>
<b>Occurrence</b>	<ul style="list-style-type: none"> <li>• Type of crime</li> <li>• Location</li> <li>• Date and time of incident</li> <li>• Was physical evidence handled by officer, suspect, or victim?</li> <li>• Disposition and chain of custody for all evidence</li> <li>• Suspect direction of travel</li> <li>• Type and description of weapons</li> <li>• Threats made with weapons</li> <li>• Direct statements made by suspect</li> <li>• Case number</li> <li>• Assisting officer's actions (and supplements, if necessary)</li> </ul>	<p>All persons involved:</p> <ul style="list-style-type: none"> <li>• Informants</li> <li>• Reporting party</li> <li>• Victims</li> <li>• Witnesses</li> <li>• Suspects, if known</li> <li>• Officers</li> <li>• Outside agencies and members of outside agencies</li> <li>• Medical personnel</li> <li>• Members of the media</li> </ul>

	<b>Basic Information</b>	<b>Additional Information</b>
<b>Suspects</b>	<ul style="list-style-type: none"> <li>• Race</li> <li>• Sex</li> <li>• Age</li> <li>• Build</li> <li>• Height</li> <li>• Weight</li> <li>• Eye color</li> <li>• Hair color</li> <li>• Hair style</li> <li>• Facial hair</li> <li>• Clothing type</li> <li>• Clothing color</li> <li>• Clothing style</li> <li>• Name and/or street name, if known</li> <li>• Unusual physical attributes, such as scars, tattoos, a limp, moles, odor, and missing teeth</li> <li>• Can the suspect be identified by the victim or witness?</li> </ul>	<ul style="list-style-type: none"> <li>• Unusual or memorable gestures</li> <li>• Speech peculiarities, such as accents, tone, pitch, or noticeable speech disorder, such as stuttering</li> <li>• Jewelry <ul style="list-style-type: none"> <li>○ Rings (identify which hand and finger)</li> <li>○ Necklaces</li> <li>○ Earrings</li> <li>○ Body piercings</li> </ul> </li> <li>• Right or left-handed <ul style="list-style-type: none"> <li>○ Which hand was dominant?</li> <li>○ Which hand held the weapon?</li> <li>○ Which hand opened a door?</li> <li>○ Where was a watch worn?</li> </ul> </li> <li>• Gang affiliation (if known)</li> </ul>
<b>Incident Specific</b>	<ul style="list-style-type: none"> <li>• Scene description and photographs (if available)</li> <li>• Point of entry</li> <li>• Point of exit</li> <li>• Description of property damage</li> <li>• Types and values of property taken</li> <li>• Description of suspect vehicle</li> <li>• Nature and location of evidence collected</li> <li>• Suspect and victim injuries</li> <li>• Unique characteristics of the crime</li> <li>• Anything else not already mentioned that the officer believes is relevant to the case</li> </ul>	

## **NOTE TAKING AND CONDUCTING FIELD INTERVIEWS**

Typically, field notes are obtained from the officer's direct observations and from field interviews with suspects, victims, and witnesses. The field interview, however, is where the officer will learn most of the information about a crime or incident. Therefore, the statements

taken during a field interview are often critical to learning about the specific facts of a case, because the existence of certain crime elements may only be revealed from the statements of witnesses, victims, and the suspects of a case.

An effective field interview should generally follow the following five step format.

1. **Separate the involved parties.** This minimizes distractions and interruptions. Separating the involved parties also focuses their attention on speaking to the officer, rather than each other, and also minimizes manipulation of witness statements by other involved parties.
2. **Establish rapport.** Be courteous, considerate, and patient. Briefly tell the person being interviewed why the interview is being conducted and describe the interview process to the individual.
3. **Listen attentively.** Ask the person what happened and allow them to talk about it freely. Let them explain it in terms that they understand. Be sure to keep the person focused on the main subject being discussed in the interview. If they begin to get off topic, guide the person back to the subject, and always use active listening skills to encourage the person to talk. Listen carefully and pay attention to the details of the incident. Do not take notes at this point in the interview, as it is a distraction to the person and your listening skills.
4. **Take notes/Ask questions.** Ask the person to repeat their account of what happened, but stop the person and ask questions for clarification, where necessary. Take notes, but write in short, simple statements, highlighting the important thoughts or ideas. Be sure to obtain accurate identification information for the person at this point and ask any additional questions that are necessary for clarification.
5. **Verify information.** Repeat specific information to the person being interviewed from the notes taken in the previous step, to ensure accuracy, and give them an opportunity to add facts. Be sure to confirm direct quotes, time relationships, weapons information, and physical descriptions of suspects. Be sure to verify any changes made in this stage.

It is important to note that while some officers may elect to record an interview with a digital voice, tape recorder, or body camera the use of a recorder may inhibit an individual from talking freely. Also, electronic devices can malfunction or fail, thereby eliminating the information from the interview. If interviews are recorded, officers should also take written notes as a backup in the event of mechanical or device failure.

## **IMPORTANT FIELD INTERVIEW SKILLS**

One of the most important skills that officers are required to have while conducting a field interview and taking field notes is determining the difference between opinions, facts, and conclusions in a statement given by a suspect or witness. Another important skill is being able to determine what information is relevant to the case or incident.

Opinions are statements that can be open to interpretation, or expresses a belief not supported by the facts of a case, while a fact is a statement that can be verified or proven by the facts of the case. A conclusion is a statement that is based upon the analysis of opinions and conclusions, and a conclusion should always be accompanied with the supporting facts and opinions.

Generally, relevant facts typically establish the facts of the case or elements of the crime. Irrelevant facts, on the other hand, usually furnish details that are not elements of the crime or provide information that may dilute the facts of the case.

## QUESTIONS ANSWERED BY AN EFFECTIVE REPORT

The facts and questions that an officer includes in his or her field notes should typically provide the foundation for an effective police report. As discussed earlier, an effective police report should always answer the questions who, what, where, when, how, and why.

If any of the six questions cannot be answered by the officer's report, the report should contain as much information as possible, as the information can prove to be vital to investigators, attorneys, and other users of the report.

The following table presents examples of the specific facts and information that can be included in the body of the report to help answer of the six questions. It is not intended to be all inclusive, but simply used as a guide. Specific crimes or incidents will require certain information that should be noted by the investigating officer in the report.

	<b>Supporting Facts/Information</b>
<b>What</b>	<ul style="list-style-type: none"> <li>• was the crime that was committed?</li> <li>• are the elements of the crime?</li> <li>• were the actions of the suspect before and after the crime?</li> <li>• actually happened?</li> <li>• do the witnesses know about it?</li> <li>• evidence was obtained?</li> <li>• was done with the evidence?</li> <li>• weapons were used?</li> <li>• action did the officers take?</li> <li>• further action should be taken?</li> <li>• knowledge, skill, or strength was needed to commit the crime?</li> <li>• other agencies were notified?</li> <li>• other agencies need to be notified?</li> </ul>
<b>When</b>	<ul style="list-style-type: none"> <li>• was the crime committed?</li> <li>• was the crime discovered?</li> <li>• were the involved parties notified?</li> <li>• did the involved parties arrive at the scene?</li> <li>• was the victim last seen?</li> <li>• was the suspect last seen?</li> <li>• did officers arrive?</li> <li>• was any arrest made?</li> <li>• did witnesses hear anything unusual?</li> <li>• did the suspect decide to commit the crime?</li> </ul>

	<b>Supporting Facts/Information</b>
<b>Where</b>	<ul style="list-style-type: none"> <li>• was the crime committed?</li> <li>• was the crime discovered?</li> <li>• was entry made?</li> <li>• was the exit?</li> <li>• was the weapon obtained that was used to commit the crime?</li> <li>• was the victim found?</li> <li>• was the suspect seen during the crime?</li> <li>• was the suspect last seen?</li> <li>• were the witnesses during the crime?</li> <li>• did the suspect live?</li> <li>• does the suspect currently live?</li> <li>• is the suspect now?</li> <li>• would the suspect likely go?</li> <li>• was the evidence found?</li> <li>• was the evidence stored?</li> </ul>
<b>Who</b>	<ul style="list-style-type: none"> <li>• are the involved parties in the incident? (i.e., victim(s), witness(es), suspect(s))</li> <li>• were the participating officers?</li> <li>• was the complainant?</li> <li>• discovered the crime?</li> <li>• saw or heard anything of importance?</li> <li>• had a motive for committing the crime?</li> <li>• committed the crime?</li> <li>• had the means to commit the crime?</li> <li>• had access to the crime scene?</li> <li>• searched for, identified, and gathered evidence?</li> </ul> <p>Also with whom...</p> <ul style="list-style-type: none"> <li>• did the victim associate?</li> <li>• did the suspect associate?</li> <li>• was the victim last seen?</li> <li>• do the witnesses associate?</li> <li>• did the suspect commit the crime?</li> </ul> <p>Additional information regarding specific people can include, but not be limited to:</p> <ul style="list-style-type: none"> <li>• phone numbers (home, cellular and work)</li> <li>• addresses (home, work, and email)</li> <li>• age and date of birth</li> <li>• social security number</li> <li>• occupations</li> <li>• physical descriptions as required</li> </ul>

	Supporting Facts/Information
How	<ul style="list-style-type: none"> <li>• was the crime committed? (e.g., force, violence, threats, etc.)</li> <li>• did the suspect leave the scene? (e.g., on foot, by car, etc.)</li> <li>• did the suspect obtain the information necessary to commit the crime?</li> <li>• was the crime discovered?</li> <li>• was entry made? (e.g., smashing, breaking, key, etc.)</li> <li>• was the weapon/tool for the crime obtained?</li> <li>• was the weapon/tool used?</li> <li>• was the arrest made?</li> <li>• much damage was done?</li> </ul>
Why (if known)	<ul style="list-style-type: none"> <li>• was the crime committed?</li> <li>• was a certain weapon/tool used?</li> <li>• was the crime reported?</li> <li>• was the crime reported late?</li> <li>• were witnesses reluctant to give information?</li> <li>• is the suspect lying?</li> <li>• did the suspect commit the crime when she/he did?</li> <li>• did the suspect commit the crime where she/he did?</li> </ul>

## FUNDAMENTAL REPORT CONTENT

As previously stated, every crime or incident is different, and as a result, each report will require different information to complete a total word picture about the incident. However, every report should have certain content elements, regardless of the crime that was committed.

The following general content elements are fundamental to an effective report; however, it should be noted that in some crimes or incidents, a specific element may not be applicable.

1. **Initial information.** This should establish how the officer became involved with the specific incident and additional background information. The initial information should also describe the officer's immediate observations and any actions they took upon arrival at the scene.
2. **Identification of the crime or incident.** Always include the facts that are necessary to show that the specific crime or incident has taken place. The report should include the common name of the crime, the statutory reference number, and the required elements necessary for the crime to be complete.
3. **Identification of the involved parties.** Regardless of the type of report, the report should **always** identify the reporting persons, victims, witnesses, and suspects, if known. Always include full legal names, address, home, work, and cellular telephone numbers. Include alternate contact information, such as work or school addresses, email addresses, and their role in the incident.
4. **Victim/witness/suspect statements.** Summary statements of all involved parties should be taken, and direct quotes used, where necessary. Statements should always include the details of the events, from their own perspective. Original Written statements are notarized by the investigating officer and included with the officer's written report.



5. **Crime scene specifics/description.** Crime scene specifics are necessary to accurately re-create the scene and events of the crime. Include photographs, where possible, and include the locations of physical evidence prior to collection. Photographs should be printed for inclusion with the report, and booked as property as evidence, where applicable. Sketches of crime scenes are another valuable tool that should be included with the officer's report.
6. **Property information.** Property information should include the color, make, model, serial number, approximate value, and full descriptions where possible. Details pertaining to stolen or recovered property, as well as property booked for safekeeping, and property booked as evidence should always be included in the report.
7. **Officer actions/observations.** Include descriptions and observations of all actions related to the incident. If multiple officers responded to a crime or incident, each officer involved is required to provide the investigating officer a supplemental report that details their own actions at the incident or crime. The supplement should be submitted for inclusion with the main investigating officer's report. All reports, whether a master report or supplemental report, should be written from the perspective of the writing officer, and detail their own personal actions and/or observations without regard to outside influences.

## RECOMMENDED GRAMMAR FOR REPORTS

An effective report must always exhibit the writer's grasp of the English language, and be relatively free of errors in sentence structure, grammar, and other writing mechanics, and the more effective the officer's command of the written language, the greater the clarity of the written report.

Due to the large number of grammatical guidelines in the English language, officers should have a basic understanding of the basic building blocks of sentence structure when writing reports.

### **Nouns**

Nouns are naming words, and could be used to identify people, places, or things.

### **Proper nouns**

Proper nouns refer to specific places persons, or things, and always should begin with a capital letter. When referring to a specific person within a report, officers should use proper nouns. After the proper noun has been used once, just the last name may be used when referring to the same person.

### **Pronouns**

Pronouns are words that substitutes for a noun or proper noun. There are two types of pronouns primarily used in report writing.

- **First person pronouns.** First person pronouns are used when referring to the officer writing the reports. Some examples are I/me/mine/my and we/our/ours/us (when riding with a beat partner). First person pronouns can also be used within quotes to refer to the person speaking (Wilson told me, "I ran as fast as I could."). Officers should always use first person pronouns when referring to themselves, by doing so, the reader has a clear understanding of the officers' actions.
- **Third person pronouns.** Third person pronouns refer to the person, place or thing being written about. Examples are he/his/him, it/its and they/their/them. Third person pronouns must always agree and clearly refer to the noun or proper noun that is directly before it.

## Tense

Since most investigative reports are written about things that have already happened, the words that are used should clearly indicate the events occurred in the past. This is expressed through the tense of the action words (or verbs) in the report. Tense can be either present or past tense.

- Present tense. Present tense verbs express an action currently taking place. For example, the phrase “I am reading this manual” is written in the present tense.
- Past tense. Past tense verbs express actions completed in the past for example, the phrase “I read this manual last week” is written in the past tense.

## Voice

The term “voice,” when used to describe a type of verb, refers to whether the verb is active or passive. Reports should always be written in the active voice, as most readers find sentences written in the active voice easier to follow and understand.

- Active voice. A verb is in the active voice when the subject of the sentence is the individual or thing that is doing or performing the action. An example would be “I gave the report form to the victim.”
- Passive voice. A verb is in the passive voice when the subject of the sentence is someone or something other than the performer of the action in the sentence. *A common indicator of passive voice is the word “by” in the sentence.* An example would be “The victim was given the report form by me.”

## **WRITING CLEARLY AND LOGICALLY**

As previously discussed, effective police reports must be organized, logical, and present all relevant information simply. An effective report must also be written in plain English to be useful and understandable for the reader.

## Paragraphs

Paragraphs are the structural units for grouping information. Regardless of whether a narrative style format or a category format is used for the investigative report, all paragraphs within the report must be clear and easy to understand.

When writing an investigative report, the first sentence (lead-in sentence) of each paragraph should clearly state the primary topic or subject of the paragraph. The sentences that follow within the paragraph should present facts, ideas, reasons, or examples that are directly related to the primary topic.

The following table presents examples of poorly organized and well organized paragraphs.

<b>Poorly Organized</b>	<b>Well Organized</b>
When we arrived, the husband let us into the house. We were responding to a 9-1-1 call. My partner and I had been dispatched to an incident of domestic violence. A woman called for help to keep her husband from beating her.	My partner and I were dispatched to a domestic violence incident after a woman dialed 9-1-1. The woman called for help because she was afraid her husband would beat her. When we arrived, the husband let us into the house.

## Transitions

Transitions are words or phrases that show relationships between thoughts, sentences, or paragraphs. By selecting appropriate transitional words, officers can help readers move smoothly and logically from detail to detail and sentence to sentence within the report.

The following table suggests a few of the possible transitional words and phrases officers may use within their reports.

Type of Transition	Words/Phrases	Examples
Time	<ul style="list-style-type: none"><li>• Immediately</li><li>• In the meantime</li><li>• At the same time</li><li>• When</li><li>• Before</li><li>• Prior to</li></ul>	Caster said he noticed the door was not completely shut, so he decided to find out why.  <b>Immediately after</b> entering the room, he saw the window was broken.
Place	<ul style="list-style-type: none"><li>• Near</li><li>• Beyond</li><li>• Next to</li><li>• Under</li><li>• Behind</li><li>• Around</li></ul>	Caster said he saw broken glass on the floor under the window.  <b>Near the</b> glass, he saw a large brick.
Order	<ul style="list-style-type: none"><li>• Finally</li><li>• In addition</li><li>• Lastly</li><li>• First</li><li>• Then</li><li>• Further</li></ul>	<b>In addition,</b> Caster saw his laptop computer was not on the desk where he left it the night before.

## Concrete vs Abstract Words

Stay away from using police jargon, phrases, and acronyms when writing reports. Reports should be written using simple, common, and concrete language whenever possible. The use of simple language can help keep reports concise and brief and addresses relevant information quickly and clearly.

The following table presents examples of abstract words and phrases, along with more concrete alternatives.

Abstract Words	Concrete Words
A number of ...	Seven...
At a high rate of speed...	75 MPH...
Appeared intoxicated...	Breath smelled of an alcoholic beverage...

<b>Abstract Words</b>	<b>Concrete Words</b>
Hostile behavior...	Repeatedly struck at officers...
Physical confrontation...	Fight...
Verbal altercation...	Argument...
Extensive record...	Six DUI offenses over two years...
Employed...	Used...
Dispute...	Argument...
Inquired...	Asked...
In the vicinity of...	Near...
Articulated...	Said, told...
Hit...	Punched, slapped or clubbed...

## **Homonyms**

Homonyms are words that sound the same but have different meanings. There are a number of frequently used words that sound alike but have completely different spellings and meanings. When writing reports, officers should ensure that they are using the correct word for what they are trying to express.

The following table identifies the most commonly confused sound-alike words.

<b>Words</b>	<b>Definitions</b>	<b>Examples</b>
Accept	To take with approval, or agree to	I accepted the medal with pride
Except	To omit or exclude; preposition meaning 'but'	We did everything except interview the witnesses.
Access	An approach, admittance, or route	There is an access road running east to west in front of the drug store.
Excess	Surplus; an amount greater than wanted	The amount of cocaine found was in excess of what had been initially reported.
Advice	Worthy suggestion or information; noun	My sergeant gave me advice on how to handle the situation.
Advise	To give suggestions, data or counsel; verb	My sergeant advised me on how to handle the situation.
Affect	To act upon or produce change or influence; verb	The suspect was affected by the pepper spray.
Effect	Result of cause; belongings; noun	Dilated pupils are a physical effect of the drug. The coroner removed the personal effects from the victim.
Allude	Make reference to	The witness alluded to the suspect's collection of guns.
Elude	To escape or evade	The suspect eluded arrest by going into a store.

<b>Words</b>	<b>Definitions</b>	<b>Examples</b>
Assure	To offer assurances	The officer assured the victim that the batterer would be jailed.
Ensure	To make certain	The officer ensured the suspect was correctly handcuffed.
Insure	To make secure or certain (as with ensure); or to guarantee life or property against risk.	The man insured his house against fire and floods.
Brake	To stop a vehicle	Her car's brakes failed, and she ran into the truck in front of her.
Break	To burglarize a home or other structure; forcibly entering or exiting a house or structure; to damage.	The officer watched the suspect break into the store.
Cite	Refer to an official document or rule as proof; verb	The district attorney cited the penal code.
Site	Place or setting of an event; noun	The officers returned to the site of the crime to gather more evidence.
Sight	Ability to see	The contraband lay on the table in plain sight.
Elicit	To draw out or forth; evoke	The officer was able to elicit a confession from the suspect.
Illicit	Something not permitted by law	The suspect had committed an illicit act.
Formally	Something done ceremoniously or in a regular, methodical fashion	The suspect was formally indicted in for the crime.
Formerly	Something that happened in the past	He was formerly a detective.
Hear	To perceive sound	The officers could hear the argument through the door.
Here	Place or location	I asked the victim to come here and answer some questions.
Its	Adjective showing possession	The car lost its rear hubcap when the officer drove over the curb.
It's	Contraction of 'it is' or 'it has'	It's been six years since the officer was hired.
Know	To be cognizant of or be acquainted with	The victim claimed that she did not know the suspect.
No	Negative	The suspect said, "No."
Pain	Strong sense of hurt	The victim screamed in pain after being Tasered.

<b>Words</b>	<b>Definitions</b>	<b>Examples</b>
Pane	Window glass set in a frame	The burglar had broken the pane to gain access to the house.
Passed	To move forward or around; to circulate	As we pursued the suspect, we passed four other vehicles on the freeway.
Past	History; ended or accomplished, beyond	The suspect had a number of past convictions.
Personal	Belonging to someone	The suspect's personal effects were booked into property.
Personnel	Company's employees	The department had a personnel meeting.
Precede	To go before in time, place or rank	The burglary preceded the rape.
Proceed	To advance, go toward	The burglary then proceeded to the bedroom.
Pride	Self-esteem	The officer took great pride in his work.
Pried	To raise, move, or force with a lever (past tense of pry)	The burglar pried the window open with a screwdriver.
Principal	Chief official; chief actor or perpetrator present at time of crime	Gary Moreno was the principal person involved in the burglary.
Principle	Rule of conduct; law of nature or scientific fact	Police officers are expected to uphold high moral principles.
Quiet	Still or silent	When we arrived at the dispute, the house was quiet.
Quite	To a great degree; completely	The suspect was quite agitated and began sweating.
Scene	Location of an event	The officers secured the crime scene.
Seen	Past tense of "to see" (sight)	The suspect was seen running from the house.
Steal	To take without permission	Robbery and theft are forms of stealing.
Steel	Strong alloy of iron	The pipe was made of steel.
Than	Introduces comparative clauses	The suspect was taller than me.
Then	Designates time (next)	The suspects then fled from the bank on foot.
There	At or in that place; to, toward, or into	Morez went there after she talked

Words	Definitions	Examples
	that place	with the officer.
They're	Short form of 'they are'	The woman said, "They're going to shoot him."
Their	Possession of them, by them	The brothers went by their home on their way to the corner.
Threw	Past tense of "throw"	She threw the vase at her husband.
Through	Motion from side to side or end to end within something	The suspect ran through the mall to evade arrest.
To	Movement toward a place, person, or thing	The victim stated he was going to the grocery store when he was stopped.
Too	Also, besides, in excessive degree	The reporting party stated that the noise was too loud for her to hear the person talking
Two	The number two (2)	The building had two entrances
Waist	Part of the body between the ribs and the hips	The suspect grabbed the victim around the waist and wrestled her to the ground.
Waste	To consume, weaken, or squander	She wasted water by washing her car twice every day.
Weak	Not strong	His use of heroin left him very weak.
Week	Seven days' duration	The suspect stalked his victim for three weeks.
Your	Belongs to a specific you or a specific person	Young heard Johnson say, "Your dog is on my property again."
You're	Short form of 'you are'	The officer said you're under arrest.
Wave	To signal	She waved to her neighbor.
Waive	To surrender or relinquish	She waived her Miranda rights.

## PROOFREADING

Proofreading may seem time-consuming, tedious, and difficult, but when writing reports where accuracy, clarity, and completeness are important, proofreading is critical. It is a difficult skill to master, yet one that cannot be overlooked.

When proofreading a report, special attention should be devoted to ensure that the following basic questions are answered:

- Are the correct crimes cited in the report?
- Is the information in the proper order?

- Are all crime elements articulated?
- Are the facts of the case correct (based on the officer's field notes)?
- Is the report well organized?
- Is all necessary information included?
- Are things said efficiently or too wordy?
- Are all conclusions supported by facts?
- Are there any gaps in logic?
- Are the names spelled correctly?

### **Proofreading Mechanics**

A report's effectiveness and an officer's credibility can be damaged by a report with too many mechanical errors. When proofreading the reports, they have written, officers should look for:

- Inappropriate use of nouns, pronouns verbs, etc.
- Vague or confusing language
- Incorrect or inappropriate use of words
- Gaps in logic or narrative flow
- Spelling errors
- Inappropriate punctuation
- Incorrect use of police, fire or EMS abbreviations
- Overuse of words, such as "that"

One of the most effective methods for proofreading the content and mechanics of any report is to slowly read the completed report aloud. When sentences are heard, it is often easier to identify mechanical errors, gaps in logical flow, skewed time sequences, incorrect verb tenses and cumbersome phrasing.



TEAGUE POLICE DEPARTMENT REPORT  
WRITING MANUAL

PART II  
INSTRUCTIONS FOR  
REPORT FORM COMPLETION

## **COMPLETION OF THE REPORT COUNTY ATTORNEY COVER SHEET**

The County Attorney cover sheet shall be completed for all reports that are to be submitted to the Freestone County Attorney for prosecution. This form is also known as a request for prosecution and includes two pages.

**NOTE:** *The responsibility for delivery of completed department reports to the County Attorney's office, in a timely manner, rests with the supervisors.*

The County Attorney cover sheet is self-explanatory in how to complete. Departmental supervisors shall ensure it is completed accurately before submission.

## **CASE STATUS INFORMATION**

### **Cleared Cases.**

A case is classified as cleared when at least one person is arrested, charged with the commission of the offense, and turned over to the court for prosecution.

A case can also be classified as exceptionally cleared when some element beyond law enforcement control prevents filing of formal charges against the offender. A report can be classified as cleared if all the following questions can be answered in the affirmative. (1) Has the investigation definitely established the identity of the offender? (2) Is there enough information to support an arrest, charge, and turning over to the court for prosecution? (3) Is the exact location of the offender known so that the subject could be taken into custody now? (4) Is there some reason outside law enforcement control that precludes arresting, charging, and prosecuting the offender (for example, suicide, death bed confession, double murder, etc.)? Examples of such clearances are:

1. Suicide of the offender. (The person who committed the offense is dead.)
2. Double murder. (Two persons kill each other.)
3. Deathbed confession. (The person who committed the offense dies after making the confession.)
4. Offender killed by police or citizen.
5. Confession by an offender who is already in law enforcement custody or serving a sentence. (This is a variation of a true clearance by arrest—the offender would not be “apprehended” but in most situations would be prosecuted on the new charge.)
6. Offender is prosecuted by state or local authorities in another city for a different offense or is prosecuted in another city or state by the federal government for an offense which may be

the same. (Law enforcement tries to return the offender for prosecution, but the other jurisdiction will not allow the release.)

7. Extradition denied.
8. Victim refuses to cooperate in the prosecution.
9. Warrant is outstanding for felon but before being arrested the offender dies. (The method of death is irrelevant.)
10. The handling of a juvenile offender either orally or by written notice to parents in instances involving minor offenses such as petty larceny. No referral is made to juvenile court as a matter of publicly accepted law enforcement policy

#### **Closed Cases.**

A case can be classified as closed when all investigation is complete, and no additional follow-up investigation can be conducted, however, suspect identification or prosecution is deemed to be remote or unlikely. In closed cases, all serialized property information must be known.

#### **Pending Cases.**

A case can be classified as pending when follow up investigation is going to be conducted by the individual officer or detectives.

#### **Unfounded Cases.**

A case is classified as unfounded when it is determined that the facts of the case are proven to be false.

#### **Other Cases.**

Cases are classified as 'other' when they are outside agency assists, or incident reports.

## COMPLETION OF THE REPORT NARRATIVE

The purpose of this section of the manual is to provide a standard guideline for the completion of all report narratives written by Teague Police Department officers.

### NARRATIVE FORMAT

The narrative format used by the department for all reports will be a chronological narrative, with categorical report headings.

Categorical headings will be in capital letters, and in bold face font. Report headings are limited to those in the table below, except in cases of driving under the influence reports.

<b><u>HEADING</u></b>	<b><u>DESCRIPTION</u></b>
Date	The date the report is written, or other action was taken by the reporting officer.
Time	The time the report is written, in 24-hour format.
Notification	A short summary of the circumstances which caused the officer to arrive at the scene of the call.
Offense	A detailed listing of the offense being investigated and/or charges being filed with the report.
Officer Actions/Observations	The actions and observations taken and noted by the officer writing the report. A scene summary may also be included under this heading. Officers can include brief statements or answers given by a victim, suspect, witness, reporting party, or other party involved in the report.
Victim Statement	<p>A detailed summary of the victim's statement to the officer writing the report.</p> <p>The victim's last name will be written in parenthesis after the heading. In cases in which there are multiple involved parties with the same last name, both the first and last name will be used.</p>
Suspect Statement	<p>A detailed summary of the suspect's statement to the officer writing the report.</p> <p>The suspect's last name will be written in parenthesis after the heading and before the beginning of their statement. In cases in which there are multiple involved parties with the same last name, both the first and last name will be used.</p>

Witness Statement	<p>A detailed summary of the witness’s statement to the officer writing the report.</p> <p>The witness’s last name will be written in parenthesis after the heading and before the beginning of their statement. In cases in which there are multiple involved parties with the same last name, both the first and last name will be used.</p>
Reporting Party Statement	<p>A detailed summary of the reporting party’s statement to the officer writing the report.</p> <p>The reporting party’s last name will be written in parenthesis after the heading and before the beginning of their statement. In cases in which there are multiple involved parties with the same last name, both the first and last name will be used.</p>
Other Party Statement	<p>A detailed summary of the any additional party’s statement to the officer writing the report.</p> <p>The additional party’s last name will be written in parenthesis after the heading and before the beginning of their statement. In cases in which there are multiple involved parties with the same last name, both the first and last name will be used.</p>
Property/Evidence	<p>A detailed listing of property stolen/missing/recovered and/or evidence observed/recovered.</p>
Recordings/Photos	<p>A detailed list of any videos (in-car, body camera, phone recordings, DVR Security footage, etc.), photos, audio recordings are made in this section. Officer should document the disposition of the items and/or the lack of having these items (“due to body camera malfunction I do not have body camera video”).</p>
Recommendations	<p>A brief summary of follow up required, or actions to be taken with the report, with a brief explanation. If further follow up is required, the explanation should detail who is going to conduct the follow up (eg, the officer writing the report, detectives, other named officer).</p>
Report Summary	<p>A final statement by the reporting officer describing the case status and/or disposition of the report. For example; “This case is cleared by arrest and is being forwarded to the Freestone County Attorney’s Office for Prosecution,” “This case is being forwarded to the Freestone County Attorney’s Office for Review,” “This case is unfounded,” “This case is pending more investigative leads,” etc.</p>

TEAGUE POLICE DEPARTMENT REPORT  
WRITING MANUAL

PART III  
SPECIFIC REPORT INFORMATION

## **SPECIFIC REPORT INFORMATION**

Different reports, such as theft reports, burglary reports, use of force reports and driving under the influence reports, should answer particular questions and specific details, based upon the report type.

Specific questions to be answered or considered for different report types are listed below.

### **Casualty/Medical Aid Reports**

While casualty reports are typically nothing more than an incident report, their importance cannot be underestimated. The potential for civil liability from incidents in which an involved party is injured can be quite high, depending upon the circumstances. As a result, the need to carefully document the incident is of an utmost necessity. The following are elements that need to be addressed in a medical aid or casualty report.

1. **Describe the scene.** Be as thorough as possible, and include any broken concrete, improper lighting, incorrect signage, or other conditions observed.
2. **Establish the timeframe of the incident.** This information is critical to impeach and rehabilitate the statements of involved parties.
3. **Take a complete statement from all parties involved.** Include statements detailing the victim's injuries and be sure to speak with the victim. Be as complete and thorough as possible, if something does not make sense, get clarification immediately, because it may be the only time the party is contacted.
4. **Get complete contact information for all parties.** Be sure to get alternate telephone numbers and email addresses, whenever possible.
5. **Canvass the area for possible witnesses.** Do not hesitate to knock on doors, if necessary.
6. **Describe any injuries or other preexisting medical conditions described by involved parties.** A thorough description contemporaneous to the incident will prevent possible statement changes later.
7. **Take photographs of the scene, and of all involved parties.** Once again, a picture is worth a thousand words.
8. **Determine if there is video of the incident.** If there is video, obtain a copy, and book it as evidence.
9. **Get medical release statements, if necessary.** Having access to medical records from the outset can sometimes prevent excessive claims later.
10. **Document the fire and medical units on scene.** If the involved party refuses medical aid, document the reason.
11. **Obtain the hospital information if the involved party is transported.** Be sure to include this information in the report.

## Theft/Burglary/Other Property Crime Reports

Theft/Burglary/ and other property crime reports should answer questions regarding modus operandi, points of entry, items taken, timeframe, and evidentiary information in order to enable investigators to link specific incidents together. The following are elements that should be addressed by an effective property crime report.

1. **Describe the scene.** Always describe the scene as it was when the victim discovered the crime, and how the scene appeared when you arrived.
2. **Establish what crime occurred.** Articulate all elements of the crime in the report.
3. **Establish the timeframe of the crime.** This information is critical to impeach and rehabilitate the statements of suspects and victims.
4. **Take a complete statement from all parties involved.** Be as complete and thorough as possible, and if something does not make sense, get clarification immediately, because it may be the only time the party is contacted.
5. **Get complete contact information for all parties.** Be sure to get alternate telephone numbers and email addresses, whenever possible. Do not list a stolen, lost, or missing telephone as the only contact information in the case.
6. **Thoroughly describe the property taken, damaged, or missing.** Be as thorough as possible and follow up with the victim or responsible if necessary, to obtain the information. Be sure to include the color, make, model, value, and serial number of items, where available. Also describe any owner applied markings, if applicable. If the item is a cellular telephone, obtain the MEID/IMEI numbers, if possible (The carrier provider often has this information).
7. **Canvass the area for witnesses.** A witness can provide suspect information or help confirm the timeframe.
8. **Look for cameras and obtain any video surveillance.** Determine if there is any video surveillance in the area, and document it in the report. Obtain copies, if possible, of the video surveillance for the timeframe of the crime, and book as evidence. If the surveillance is only of entrances and exits, obtain it anyway,
9. **Describe the point of entry, point of exit, and mode of theft, if possible.** Criminals are creatures of habit, as most humans are, and will typically use the same methods to commit certain types of crimes.
10. **Ask the victim if any other people had access or permission to take their property.** This can give a starting point, and may help narrow the timeframe of the crime.
11. **Photograph the scene and ask the victim if they have any pictures of their property.** A picture is worth a thousand words, every time.
12. **Look for, obtain, and book all evidence, or perceived evidence.** Look for the ninja rocks around a vehicle burglary with a window smash or look for the cut cable lock in the bushes. Do not forget to try to lift latent fingerprints, regardless of the value of the stolen property. All it takes is one print to make a case.
13. **Talk to the victim about future crime prevention techniques, if necessary.** Mention LoJack for computers, engraving, and registration of bicycles, not leaving property unattended...an ounce of prevention is worth a pound of cure.



## Use of Force Reports

Use of force reports often are subjected to a significant amount of scrutiny by both the criminal and civil courts. For this reason, specific questions and facts should be answered in a report documenting use of force. The following are elements that need to be addressed in a use of force report.

1. **Explain the probable cause or reasonable suspicion for the contact.** Clearly articulate the purpose of the stop. Be sure to include an accurate, detailed sequence of events leading up to the stop or contact.
2. **State your facts then make the conclusions.** It is better to explain the facts of what is seen, and then explain or present a conclusion. For example, do not say 'the subject appeared angry.' Explain the subject's stance, visible or expressed emotions, the subject's present ability to complete a perceived threat, and the words used by the subject. After explaining this information, conclude the description with 'the subject appeared angry.'
3. **Past experiences are important indicators of probable future behavior.** Include past experiences at the call location, past experiences with the suspect, and knowledge relayed to by other officers or dispatch. It is common for people to act in accordance with recent past behavior, so a violent subject contacted at a particular location last week, is likely a violent subject this week.
4. **Explain any objective symptoms that are observed.** This includes observed emotions, aggressive behavior or symptoms of drug and alcohol intoxication. Once again, be sure to lay out the facts before drawing the conclusions.
5. **Present ability.** Explain the suspects' present ability to delay, obstruct, cause injury, or commit the perceived threat. What is their physical presence and what ability do they have to carry out their behaviors or threats? How far away are they? What actions have been taken for officer safety, suspect containment, or scene control? If there is some distance between the officer and suspect, explain why the distance is a factor. Many people reading a use of force report may not understand that a suspect can still attack from across the street. Also, do not forget to compare and contrast suspect size and strength with the responding officers' size and strength; both are important factors that need to be explained in order to demonstrate the need for and the type of force used.
6. **Describe the physical stance of the suspect.** Explain the suspect's body language by describing the physical stance. Does the body language telegraph their intentions to the point where it is obvious what is coming next?
7. **What words are spoken by the officer and suspect.** Explain your verbal efforts (De-Escalation techniques) to get the person to stop doing what they are doing and explain their verbal responses. In other words, what did you say and do to prevent further problems? What did they say and do to continue creating the obstructions or delays?
8. **What actions were taken in response to the suspects words or actions.** Explain any use of force and whether it was effective or not effective. If there is any physical violence whatsoever, regardless of whether injuries appear, always take photographs, and document this fact!
9. **Identify which force option was used and why it was chosen over others.** Explain what options are available, and clearly explain why the force option used was chosen and why.
10. **Estimate strikes unless facts indicate you know for sure.** There is no harm in watching the video while writing.
11. **Always presume a videotape is being made of the event.** With the prevalence of video enabled telephones, cameras, and other video capture devices, video of the event is highly likely. Take no action that is not justified, and never neglect to document all aspects of the arrest or incident.

12. **State when medical assistance was called and why.** Remember, police cars are used to transport prisoners, not people in medical need. If possible, bring medical aid to you. If it does not come to you, explain why it did not.
13. **Take pictures of the scene and the suspect. When in doubt, take more pictures.** There is never enough; one picture is worth a thousand words. However, photographs should not be used in place of a written description of the injuries by the reporting officer.
14. **Contact all witnesses and document all contacts and attempts.** Contacting witnesses demonstrates professionalism and integrity, and also indicates an attempt to fully document the incident, regardless of whether witnesses support the use of force incident or not. Do not forget to canvass the area for witnesses!
15. **Document the number of officers, suspects, and bystanders at the scene.** Provide their names if possible, especially if they are hostile towards law enforcement. Did they say or do anything that affected the situation?
16. **Document the proximity to potential weapons.** A potential weapon is anything that can be used to hurt or cause injury, such as a stick, knives, chairs, rocks, etc.
17. **Document any special training.** Include defensive tactics training that you have had, or if the suspect has a special understanding of defensive skills.
18. **Document the duration of the incident.** Was anyone exhausted or injured during the incident.
19. **Discuss any mental illness or drug usage.** Mental illness or drug usage can explain pain tolerance or irrational responses.
20. **Describe any environmental factors that affected your decision-making process.** Were there any environmental factors, such as rain or darkness that affected your decision to use a particular force option?
21. **Document the danger to the public created by this incident.** Include any past, present, or future danger that you considered as the incident unfolded. Discuss each as known at the time of the incident.
22. **Proofread the final report with another officer.** Describe the use of force situation to an objective listener, and have the person review the report, and have them point out any logic, grammatical, or missing points that may have been left out or may have been inadequately described in the report.

### **Sexual Assault/Domestic Violence/Battery/Other Crimes Against Persons**

Sexual assaults, domestic violence, battery, and other crimes against persons are some of the most serious crimes to which officers respond. The following are elements that should be addressed by an effective report of a sexual assault, domestic violence, battery, or other crime against persons.

1. **Describe the scene.** Always describe the scene as it was when the victim discovered the crime, and how the scene appeared when you arrived. Include distances, locations of parties, lighting conditions...anything that may be considered relevant to the incident.
2. **Establish the timeframe of the crime.** This information is critical to impeach and/or sustain the statements of suspects and victims.
3. **Take a complete statement from all parties involved.** Be as complete and thorough as possible, and if something does not make sense, get clarification immediately, because it may be the only time the party is contacted.
4. **Get complete contact information for all parties.** Be sure to get alternate telephone numbers and email addresses, whenever possible. Do not list a stolen, lost or missing telephone as the only contact information in the case.
5. **Establish the relationships between all parties involved.** Doing so is important, because it may establish specific crimes, motivations, and circumstances involved in the incident.

6. **Establish what crimes occurred.** Doing so establishes probable cause for arrest. Always ensure all elements of the crime are clearly articulated.
7. **Document any injuries.** Take photographs, and obtain follow up photographs, if necessary. Be sure to obtain a medical release waiver, wherever possible. If medical transport is necessary, document the hospital.
8. **Collect any clothing and bedding involved and book the items as evidence.** Photograph the items before booking.
9. **Document all alcohol and drug involvement by all parties.** Include the amounts, types of drugs, and frequency of ingestion during the incident, and determine past alcohol and drug usage history. Also determine if any of the parties have used alcohol or drugs together before. Be sure to document the approximate intoxication level of all involved parties, where possible.
10. **Canvass the area for witnesses.** Check other rooms, residences, or businesses nearby.
11. **Determine if there is video surveillance.** If so, obtain copies and book into evidence immediately. If the video surveillance is only of the entrance or exit of a building, obtain a copy anyway, even if the crime is not visible on the video.
12. **Consider a pretext telephone call in all sexual assault cases.** Attempt to do so prior to contacting the suspect in the case.
13. **Offer confidentiality to the victim, and offer an advocate, if applicable.** Never forget that victims of sexual assault and other crimes are eligible for confidentiality and have the right to an advocate. They may also utilize a pseudonym in the report, to protect their identity.
14. **If the crime involves sexual assault, encourage the victim to undergo an evidentiary exam.** Be sure to adequately explain the purpose of the exam and allow the victim to make the decision.
15. **Record interviews.** Recording interviews ties a victim, suspect or witness to a specific statement, and limits later redactions or retractions of statements.
16. **Consider the possible defenses that can be used by the suspect.** When a possible defense is noted, try to rule out the defense though physical evidence, or follow up questioning.
17. **Do not jump to conclusions regarding the truthfulness of the victim, suspect or witness.** Doing so will bias the initial investigation. Always assume that the crime happened, unless there is strong evidence that indicates otherwise.
18. **Complete the Magistrate Information Sheet.** This is required for Emergency Protective Orders to be issued at the time of arraignment.
19. **Provide and document issuance of victim notices.** Texas Statutes mandate giving family violence victims certain information. It is incumbent on officer to document their compliance with these requirements.

### **Driving While Intoxicated (DWI) Reports**

Driving under the influence reports are often subjected to significant scrutiny, due to the social and financial impact upon arrestees because of a conviction. The following are elements that should be addressed by an effective driving while Intoxicated report.

*Note: Current DWI reporting standards encourage each field sobriety test be documented in the report narrative.*

1. **Specify the probable cause for the stop/contact, and all observations made prior to the traffic stop.** Be sure to name specific vehicle code sections, and if appropriate, name multiple violations. Doing so will limit the ability for the defense to challenge the probable cause for the initial traffic stop. Document the time of the stop and current weather conditions in the report!
2. **Identify any passengers, or other parties involved in the case.** Passengers or other involved parties are witnesses, so be sure to document and treat them as such.

3. **Describe specific objective symptoms observed.** If the case ends in a jury trial, most jurors will not understand what objective symptoms of alcohol intoxication are without an adequate description. Use terms such as 'red, glassy eyes', 'thick, slurred speech', and 'odor of an alcoholic beverage'. Provide detailed descriptions of observations of intoxication.
4. **List each standardized field sobriety test under its own heading.** Describe the administration of the test, and the results, documenting any observed errors where the subject did not perform the test as demonstrated/instructed.
5. **Be sure to demonstrate each standardized field sobriety test prior to administration.** Document the demonstration, and if the subject had any questions.
6. **Do not say the subject failed the standardized field sobriety test.** Always say the subject did not perform the test as demonstrated/instructed. Standardized field sobriety tests are based on the number and percentages of errors observed to determine the likelihood of intoxication. Thus, they are not a pass/fail test.
7. **Always perform at least three standardized field sobriety tests.** Always administer the three standardized field sobriety tests: Horizontal Gaze Nystagmus, Walk and Turn, and One Leg Stand. Other tests include the Rhomberg Balance, Finger to Nose, Finger touch, etc. Officers should never administer tests they have not been trained/certified to administer.
8. **Include the results of the Intoxilyzer test results in the report.** Attach the intoxilyzer printout to the report, in addition to including the results in the narrative. Include the time the intoxilyzer test was administered and who administered the test.
9. **Document the phlebotomist's actions if a blood test is chosen.** Be sure to document the phlebotomist cleaning the subject's arm, and the type of solution used (usually povidone iodine), and the disposition of the vials of blood. DWI Blood kits are to be immediately mailed to the appropriate Texas DPS Crime Lab for analysis. Completion instructions and required submission forms are included inside the kit.
10. **Document the storage location all property in the report.** Be sure to include personal property, as well as the vehicle. Provide a property receipt, if necessary/required.
11. **Document the booking time of the subject in the report.** Documenting the booking time takes the report full circle, from the time of stop, until time of booking.
12. **Send Texas Department of Public Safety Driver Improvement and Control Division a copy of the report, along with the required DIC forms.** This should be completed immediately after the arrest has been made and the report is approved.