TEXARKANA, TEXAS POLICE DEPARTMENT
GENERAL ORDERS MANUAL

Effective Date **February 11, 2020**	*Amended Date*	*Directive* **5.01.2**	
Subject **TLETS Terminal, Mobile Data Terminal and CJIS Security**			
Reference			
Distribution **All Personnel** **City Manager** **City Attorney**	*TPCA Best Practices Recognition Program Reference* **None**	*Review Date*	*Pages* **2**

This Operations Directive is for internal use only and does not enhance an officer's civil or criminal liability in any way. It should not be construed as a creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violations of this Operations Directive, if proven, may only form the basis for a complaint by this Department, and only in a non-judicial administrative setting.

SECTION 1 PURPOSE

To establish guidelines for use and security of the department issued TLETS Terminal, Mobile Data Terminal (MDT) equipment and related CJIS information.

SECTION 2 POLICY

It shall be the policy of the 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.

SECTION 3 DEFINITIONS

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.

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
.

SECURE LOCATION -This term includes the areas of the 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.

NON-SECURE LOCATON -This term includes all locations not defined as "secure location" above.

SECTION 4 PROCEDURES

1. CJIS, TLETS, TCIC and NCIC data shall be accessed ONLY from secure locations, as defined above.

2. 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.
3. Maintain a roster and/or agency-issued credentials (officer badge, access card, etc) of authorized personnel with unescorted access into physically secure areas.
4. 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.
5. 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.
6. 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.
7. 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.
8. The Department shall keep a list of all MDT IDs and contact(s) so that devices can be promptly disabled, should the need arise.
9. The local CJIS network equipment shall be located in a physically secure location.
10. All law enforcement vehicles containing MDTs shall be securely locked when not in use.
11. 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
12. 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.
13. No personal hardware (PC, laptop, etc) or software shall be allowed on the agency's TLETS network.
14. No publicly accessible computers shall be allowed on the agency's TLETS network.
15. The agency shall authorize and control information system-related items entering and exiting the physically secure location.
16. The agency shall establish a Security Alert and Advisories process.

SECTION 5 RESPONSIBILITY

1. All members of the Department shall know and comply with all aspects of this directive.

2. All division commanders and supervisory personnel are responsible for ensuring compliance with the provisions and intent of this directive.