# Lake Worth Police Department
## *Policy 9.03 – TLETS Terminal, MDT & CJIS Security*
Effective Date: January 30, 2023 || Replaces: N/A
Last Reviewed: July 29, 2025 || Next Review: July 29, 2027
Reference(s): N/A

Approved By: _J.T. Manoushagian_
Chief of Police

## I. POLICY

All members of the Lake Worth Police Department shall 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 policy.

## II. PURPOSE

The purpose of this policy is to establish guidelines for use and security of the department issued TLETS terminal, mobile data terminal (MDT) equipment and related CJIS information.

## III. DEFINITION

1. 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.

2. 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.

3. Secure location - This term includes the areas of the Lake Worth 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.

4. Non-secure location - This term includes all locations not defined as "secure location" above.

## IV. 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 documented security awareness training within six months of appointment or employment and thereafter at least every two years, in accordance with CJIS policy.

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. Changes in authorized personnel (creating, activating, modifying, disabling & removing accounts) will be immediately reported to TCIC training section. Any time the user/ operator list is reviewed, it shall be documented.

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 Lake Worth Police 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. 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.

17. Failure to comply with this policy can result in disciplinary action or termination.

## V. SUPERVISORY/ INFORMATION TECHNOLOGY BEST PRACTICES

1. All members of the department who serve in a supervisory capacity, along with information technology personnel (including those employed as contractors by the City of Lake Worth), shall periodically:

a. Check to ensure servers/ terminals/ MDTs connected to the CJIS network are receiving the latest updates in regard to 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. 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. 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. Check pertinent documents to ensure they are up to date. Take appropriate action such as making editing changes or replacement if required.