The Tarrant County College District
Police Department

GENERAL ORDER

SUBJECT **Criminal Justice Information System Security Policy**	GENERAL ORDER NUMBER **427.00**
SYSTEM STANDARDS	EFFECTIVE DATE **November 10, 2021**
	REVISION DATE **April 7, 2023**
APPROVAL **Shaun Williams, Chief of Police**	PAGES **3**

Policy Statement - It shall be the policy of Tarrant County College Police Department to protect the integrity of the CJIS database and all data and information obtained through use of Mobile Data Computers (MDCs), and/or hard-wired terminals by strictly following the procedures outlined in this protocol.

Purpose - To establish guidelines for use and security of the department issued equipment, Mobile Data Computers (MDCs), workstations, and related CJIS information. Failure to comply with this policy is subject to disciplinary action up to and including termination.

219.01 – DEFINITIONS

AES – Advanced **E**ncryption **S**tandard

CJIS – Criminal **J**ustice **I**nformation **S**ervices

MDC – **M**obile **D**ata **C**omputer this term includes all laptop computers that have access, via wireless or hardwired network, to TLETS, TCIC, NCIC, or any law enforcement database.

Non-secure location – this term includes all locations not defined as ***"secure location"*** above.

NSA – National **S**ecurity **A**gency

Secure location – this term includes the areas of Tarrant County College Police Department that are not open to the public and have been properly marked by ***"Authorized Personnel Only"*** signs. This term also includes official police vehicles that are locked and/or attended by authorized sworn police personnel.

TAC – Terminal **A**gency **C**oordinator

TCIC/NCIC – Texas **C**rime **I**nformation **S**ystem **/ N**ational **C**rime **I**nformation **S**ystem

TLETS – Texas **L**aw **E**nforcement **T**elecommunications **S**ystem

219.02 – PROCEDURE

1. Fingerprint-based record checks are conducted prior to employment or assignment for all agency employees, including support personnel and cleaning staff.

2. Each person authorized to access TLETS and CJIS data shall receive security awareness training within six months of appointment or employment and thereafter, in accordance with CJIS and TLETS policies. This training may be completed by an in-person class, nexTest, and CJIS Online.

3. The terminated user's/contractor's accounts are disabled within 30 minutes of notification of termination. Passwords to all accounts in which the terminated user/contractor had access are changed. All keys are confiscated at the time of termination. TCIC training is notified within 24 hours. DPS is emailed requesting deactivation of TLETS ID. The email includes the terminated user's name and date of severance.

4. Visitors to secure areas shall be escorted by authorized personnel.

5. All printouts of CJIS data shall promptly be filed with the corresponding incident records. Otherwise, such printouts shall be promptly shredded using a crosscut shredder. All secondary dissemination is signed for and reported to the TAC**.**

6. No CJIS data will be saved to any USB drive, shared server drive, CD, floppy, internal, or external hard drives or emailed**.**

7. The Department shall keep a list of all Device IDs and vendor telephone numbers so that devices can be promptly disabled should the need arise**.**

8. CJIS, TLETS, TCIC, and NCIC data shall be accessed ONLY from secure locations as defined in definitions above. MDCs are never accessed in non-secure locations. Example: Not accessed at coffee shops, restaurants, the officer's home, etc.

9. All doors to buildings or rooms that have CJIS data are locked and posted as Restricted Areas as stated in definitions above**.**

10. The local CJIS network equipment room shall be securely locked when not occupied**.**

11. All police vehicles containing MDCs shall be securely locked when not in use.

12. When transporting non-law enforcement personnel in police vehicles, officers will close the screen of the MDC or position it in a manner that will prevent unauthorized viewing of data. Visitors are required to sit on the right side of the vehicle**.**

13. Servers, PCs, and MDC operating systems are supported by the manufacturer and maintained by the agency's internal IT department or contracted IT vendor. The operating systems are updated as released by the manufacturer**.**

14. All equipment accessing CJIS data shall have anti-virus software installed and updated automatically. This virus update is performed at a minimum of every 30 days**.**

15. Network firewall system is never at end of life and updated as released by manufacturer. MDCs firewall shall be always enabled**.**

16. All unused user or system accounts will be disabled. All vendor default passwords will be changed prior to the firewall going online**.**

17. It is policy to never share user IDs**.**

18. All interface passwords will meet CJIS requirements:

    a. Passwords shall be a minimum of 12 characters on systems procured after September 30, 2005 and on all systems by September 30, 2010
    b. Passwords shall not be a dictionary word or a proper name.
    c. Passwords and User IDs shall not be the same.
    d. Passwords shall be changed every 90 days**.**

- **e.** All systems procured after September 30, 2005 shall prevent password reuse of the last 10 passwords**.**
- **f.** Passwords shall not be transmitted in the clear outside the secure domain**.**

19. Changes in authorized personnel will be immediately reported to TCIC training within 24 hours. Users will be disabled within 30 minutes**.**

20. The policy for IOS/Firmware updates is: Updates are installed as deemed appropriate and checked for monthly by the agency's internal IT department, TAC, or contracted IT vendor. Firmware and software updates are downloaded to the server as soon as released by the manufacturer. Workstations and MDCs are updated automatically. Virus protection is checked daily and updated as soon as released by the manufacturer**.**

21. All storage media containing or used for CJIS that is no longer used shall be NSA-Level-Sanitized using methodology that over-writes all data in five iterations and then the disk shall be physically destroyed**.**

22. It is not the agency's policy to share equipment. But, if equipment is moved from one user to another within the same department in the agency, it is done ONLY after being wiped clean and initialized. The moved equipment will be documented in an equipment log**.**

23. It is the agency's policy to use a minimum of 128-bit AES encryption**.**

24. It is the agency's policy to keep a log of the FIPS 140-2 certificates**.**

25. MDCs are removed and secured by the police officer when the patrol cars are out of service or out for maintenance**.**

26. It is the agency's policy to disable all network services when not needed. A log is kept of allowed network services**.**

27. It is the agency's policy to keep all MDCs software current. The operating system is updated as released by the manufacturer. MDC firewall shall be always enabled**.**

28. It is the agency's policy to lock the computer screen when departing the immediate area**.**

29. It is the agency's policy that non-law enforcement personnel cannot communicate to law enforcement devices on the network. A manageable switch is common, but it is segmented**.**

30. It is the agency's policy to NOT connect personal equipment to the Law Enforcement Network. Additionally, employees shall not use personal devices to capture any data displayed or retrieved from the Law Enforcement Network**.**

31. The use of the MDC's is restricted to official law enforcement purposes only. The use of an MDC for non-law enforcement purposes, including but not limited to, personal use of the web browser, watching videos, or playing games is strictly prohibited**.**

32. It shall be the responsibility of each authorized user to report any violations of this security policy to the TAC**.**