Fitchburg State University Police Department

Subject: **MOBILE DATA TERMINALS** Reference: MPAC: 41.3.7 Rescinds: Section 3	
Effective Date: June 30,2019	**Review Date:**
By Order of: Michael J Cloutier, Chief of Police	

General Order

11.3.4

PURPOSE:

The Purpose of the General Order is to Comply with CJIS Security Policy, Fitchburg State University Technology Policies.

POLICY:

Fitchburg State University Police Department will ensure that all Mobile Data Terminals used in the cruisers are used in a manner that complies with State Law, University policies, and policies of the Criminal Justice Information System.

DEFINITIONS:

A. **MDT- Mobile-Date Terminal:** a cruiser mounted or otherwise portable computer used by trained and certified department members for purposes of accessing CJIS, CHSB, LEAPS records, police department information systems or other available information via secure access to various information bureaus.

B. **CJIS-Criminal History:** the computerized network, services and applications that offers law enforcement agencies within the state and nationally secure access to state and interstate criminal history, driver and vehicle records, restraining orders and other important confidential data.

C. **CHSB-Criminal History Systems Board**: the state agency responsible for maintaining the state's law enforcement data communications network and systems for the processing and dissemination of C.O.R.I. to authorized entities and persons.

D. **C.O.R.I-Criminal Offender Record Information:** Records and data in any communicable form compiled by a criminal justice agency which concern an identifiable individual and relate to the nature or disposition of a criminal charge, an arrest, a pre-trial proceeding, other judicial proceedings, sentencing, incarceration, rehabilitation, or release.

PROCEDURE:

A. User Access:

1. All users are issued a login and password, are responsible for maintaining security of the password, and should never share them with anyone.

2. Employees authorized to query Board of Probation (BOP) checks must have a user name and password and be trained to at least the "Admin. and Inquiry" level of use. A user name and password will be issued upon hire and prior to access any CJIS terminals or the department Record Management System (RMS) and Computer Aided Dispatch (CAD) system.

B. Prohibited:

1. Only authorized software may be run on mobile computers, unauthorized software programs or files may not be introduced into agency computers.

2. Authorized software may not be manipulated or altered on any agency-owned mobile, desktop. Modifying computer settings, such as changing windows is prohibited.

3. Accessing the internet for any purposes or unauthorized reasons is prohibited with the exception of:
   i. RAVE Mobile Command View

C. Use:

1. At the beginning of the shift, employees shall check the MDT while completing their routine vehicle checks. Damaged equipment must be reported to a Supervisor immediately.

2. Employees shall log onto the assigned MDT and shall remain active on the system for their entire tour. If any problems are encountered, they shall report same immediately, reporting that the equipment is inoperative. All operational issues shall be directed to the Administrative Lieutenant.

3. All mobile computing transactions must conform to FCC guidelines regarding radio transmissions and shall not contain improper language or subject matter.

4. Car to car chat shall be limited to communications which is relevant to police activity, and is subject to random review by supervisors.

5. All motor vehicle stops and field interviews shall be radioed into dispatch to ensure officer safety.

6. Some MDT's programs are equipped with an audible alarm so that officers are notified of pertinent messages or announcements. The audible alarm setting on all terminals shall be left on. No officer shall mute, turn off or disable the alarm(s) or alter the MDT's volume.

7. Officers who obtain actionable CJIS information through the MDT such as "hit"(warrant, revoked license or registration) must have the query run through dispatch to obtain a paper copy of the "hit" and to confirm accuracy.

8. The MDT is not to be used by an officer while operating a vehicle while the vehicle is in motion, as this may divert the officer's attention from the safe operation of the vehicle. Such queries should be run through dispatch.

9. No food, beverage or any other substance that may inflict damage will be placed on or near MDT.

10. Laptop screens should be cleaned with a soft, clean cloth, such as a micro fiber cloth. Use of cleaning solvents and liquid-based products on the computer is prohibited, as they often cause a hazing or damage to the screen. If further cleaning is required, notify the Administrative Lieutenant.

11. At the end of each tour, officers should log off and turn the MDT off.

12. Cruisers equipped with power switches on the laptop stand shall shut the power off the laptop stand if cruiser is parked for a prolonged period of time.

13. No USBs, flash drives, thumb drives or charging devices should be plugged into a MDT or MDT stand.

D. Security:

1. All cruisers equipped with a MDT shall be locked whenever unoccupied.

2. MDT's should be removed from any vehicle which is anticipated to be out of service for more than 2 days, or is taken to a service for repair.

3. If an MDT computer, or accessory is discovered to be lost or stolen, this shall be reported immediately to a supervisor, who shall take the necessary steps to render access of the device to the network inaccessible.

4. Any user who finds a potential lapse in security on any system shall be obligated to report the potential lapse forthwith to a Supervisor.

5. Security incident which violate confidentiality, integrity, or availability of data must be reported to a Supervisor for contact with CHSB

6. All Laptops shall be closed or in a lowered position when not in use.

E. Training:

1. All employees using the MDT's shall be trained on their use during the Field Training Program on the use of the computer and software applications they are to use.
2. CJIS users are required to be trained, tested, and certified, at the minimum, to the Admin. and Query level of use.

F. Data Log Files:

1. A transaction log of CJIS queries and responses must be maintained pursuant to 3.8.1 of the CJIS user agreement. Files must be maintained for at least 2 years and must be available to CHSB upon their request.

2. Mobile communications, data queries, and car to car chat functions are logged by the mobile software. These communications and logs may be public records and may have to be released upon receipt of a public records request.

3. A monthly query of all CJIS logs will be run and saved on the I Drive.

Approvals:

M. J. Cla

Chief of Police

8/13/19

Date