
	<b>Florida State University Police Department</b>	
<b>MOBILE DATA TERMINALS (MDT)</b>		
Revision Effective Date: 09/05/17	<b>General Order 1108</b>	Attachments: None
Rescinds/Amends: 10-34B (08/11/10), 04-200-134	Distribution: Department-Wide	CFA Reference: 32.01
	Pages: 4	

**Policy - Mobile Data Computer (MDT) Systems**

This general order establishes guidelines governing the use and maintenance of Mobile Data Terminals (MDT).

**Procedure**

**A. Use of the MDT**

1. The use of the MDT must be in support of law enforcement and associated information exchange in the form of dispatch, incident report completion, e-mail, NCIC/FCIC, NLETS, CJIS, and DHSMV data. MDTs are to be used for Departmental business and in accordance with this general order, General Order titled, "Communication Procedures", General Order, titled, "Communication Facilities and Equipment" and General Order titled, "Computer Hardware and Software".
2. The MDT docking station shall not be adjusted, other than allowed by the manufacturer, without prior approval by the Lieutenant for Uniform Operations.
3. For officer safety purposes, the MDT should only be used when the vehicle is stopped.

**B. Security of the MDT**

1. Each MDT will have virus protection software installed and activated [CFA 32.01 C]. When a virus is detected, operation of the computer will stop until authorized staff from the FSU Office of Technology Integration (OTI) can evaluate the threat and eradicate the virus.
2. The following procedure shall be followed when the vehicle is going to be unattended or an unauthorized person, i.e., prisoner, passenger, general public, etc., could possibly view unprotected material:
  - a. Minimize the screen, close the MDT monitor or log off.
3. The MDT shall remain locked into the docking station when the vehicle is in motion.

4. Users of the MDT's will not share their password or use another's password. [CFA 32.01 E]

### **C. Rights to Privacy**

1. Any NCIC/FCIC information received from an MDT is to be considered as confidential not to be divulged to any non-law enforcement personnel [CFA 32.01 D].
2. No member has any expectation of privacy for any communication or use of the MDT. All electronic communications by law enforcement agencies are considered as public records.

### **D. Data Tracking**

1. All data accessed and opened by each individual's user account, e.g., e-mail, internet, FCIC/NCIC, is tagged and monitored by FDLE and network-tracking software.
2. Use of MDT messaging may be closely monitored to curtail inappropriate transmissions.
3. Unauthorized use of MDT messaging may be grounds for discipline and/or revocation of privileges for computer use.
4. All communication and information accessible by the MDT shall be considered official Departmental communications and subject to Florida's public record laws.
5. No statutorily-protected personal information of any agency member shall appear on any MDT transmissions.
6. Any illegal or unauthorized activities concerning the retrieval of FCIC/NCIC information may result in civil litigation and/or criminal prosecution.
7. Each agency member approved to use an MDT shall be issued a secure password. This will allow each MDT to directly e-mail another MDT or computer. The messaging is to be used for official purposes only.
8. No transmissions of any kind shall contain inflammatory terms, profanity, sexual comments or innuendo, or derogatory racial terms.
9. FCIC/NCIC or DHSMV checks for warrants, vehicle registrations, and driver license status may be performed by personnel certified to use the MDT. Anytime a "hit" is received, the officer must immediately notify Communications by radio of its receipt and request confirmation and back-up if necessary.

### **E. NCIC/FCIC/JIS Access.**

1. Only those employees who are authorized and have successfully completed the necessary FCIC/NCIC training may utilize computers having FCIC/NCIC access [CFA 32.01 D].
2. Due to the sensitive nature of the data available on the MDT and the corresponding links with other systems, the following guidelines are established:

- a. Access to NCIC/FCIC information shall be in accordance with current rules and regulations established by FDLE and in accordance with the provisions of General Order titled "Communications Procedures".
- b. Access to the local Justice Information System (JIS) will be restricted to law enforcement only. Information obtained from JIS is confidential and can be used for law enforcement purposes only.
- c. No information shall be obtained for personal gain of the use or an acquaintance. Any such attempt shall result in disciplinary action—up to and including criminal prosecution.
- d. All data processed and accessed by the MDT, including car-to-car e-mail messaging and internet accessing, is subject to monitoring and random inspection.

## Glossary

**Authorized User** – An FSU PD employee utilizing an MDT for the purpose of information exchange, storage, or reporting. The employee will have been properly trained, certified, and issued a user name and password.

**DHSMV** – Department of Highway Safety and Motor Vehicles.

**FCIC** – Florida Crime Information Center managed by FDLE.

**Field Use** – Any use of an MDT for completion of forms or procedures, including those procedures where the MDT is connected to a network via wireless media.

**JIS** – Justice Information System, managed by the Leon County courts, providing local criminal justice information to authorized local agencies and users.

**Mobile Data Computer (MDT)** - A laptop computer, usually mounted within a police vehicle, issued for the purpose of field reporting, data collection, driver license checks, wanted person checks, or to serve any other legitimate law enforcement information-request/sharing function.

**NCIC** – National Crime Information Center managed by the FBI.

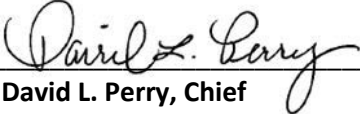
**Software** – Coded instructions that enable a computer user to operate numerous functional programs, such as e-mail messaging, internet access, report-writing, NCIC/FCIC access, etc.

**Indexing.** This general order shall be indexed as:

Communications, Computer-based  
Communications, Authorizations  
Communications, Restrictions  
Communications, Security  
E-mail, Authorizations  
E-mail, Restrictions  
FCIC  
JIS  
Internet, Access  
Mobile Data Computer (MDT)  
NCIC  
Training, MDT Usage

MTC 09/05/17 Filed: General Order 1108

Title: Mobile Data Terminal

Approved:   
David L. Perry, Chief

Effective Date: 09/05/17