


FLORIDA HIGHWAY PATROL

POLICY MANUAL

	SUBJECT MOBILE DATA COMPUTERS	POLICY NUMBER 14.03
		ISSUE DATE 05/01/01
		REVISION DATE 02/13/19
		TOTAL PAGES 6

14.03.01 PURPOSE

The Florida Highway Patrol provides each member guidelines and regulations governing the safe use of mobile data computers in FHP vehicles and vehicles utilized by FHP personnel in the performance of their assigned duties.

14.03.02 DEFINITIONS

MOBILE DATA COMPUTER (MDC) - A vehicle-based computer that provides for dispatching, car-to-car communications, and criminal justice database inquiries.

14.03.03 OBJECTIVES

To increase the efficiency and effectiveness of employees assigned to patrol duties.

14.03.04 PROCEDURES

A. ASSIGNMENT, SECURITY, AND STORAGE OF EQUIPMENT

1. Assignment of Equipment

- a. MDCs will be issued in accordance with DHSMV inventory control procedures
- b. MDCs will be installed in a manner that does not interfere with any occupant restraint devices (air bags and seatbelts). Only authorized personnel shall install or move assigned equipment.

NOTE: Members shall not modify the MDC, the MDC hardware or their printers under any circumstance. This includes, but is not limited to, removing parts, adding personally purchased hardware or modifications to any part of the system in general. Members are not to affix any decals or stickers to any component which make up the MDC or printer.

Violations of this directive may result in disciplinary action and may include the requirement to reimburse the Agency for any and all damages resulting from such modification(s).

- c. Employees are responsible for the care and security of each piece of equipment assigned to them or to their assigned vehicle.
- d. Employees are accountable for issued MDC equipment and will obtain written receipt for any item returned or exchanged.
- e. Employees will be provided with and sign acknowledging receipt of DHSMV Policies #8.01, Computer Security and #8.03, Personal Computer Use and Internet Access, prior to or upon issuance of an MDC.

2. End-of-Shift Removal and Storage of Equipment

- a. Following their shift, if the employee's vehicle will be secured in a locked garage, all MDC equipment may remain in the vehicle.
- b. If an employee's vehicle will not be secured in a locked garage, the MDC will be removed from the vehicle and stored in their residence or locked office.

NOTE: Due to the sensitivity of the equipment to extremes in temperature, MDC equipment is not to be stored in the trunk of an automobile.

3. When the employee is patrolling on-duty, the MDC will be securely mounted in the docking device in the vehicle.

4. Unattended Vehicles

- a. Vehicles will be locked when left unattended.
- b. Employees will use every precaution to safeguard equipment when the equipment is not in their immediate possession.
 - (1) Employees will, if necessary, remove the MDC from the vehicle.
 - (2) Any MDC that is left in an unattended vehicle must be locked in the docking device and the docking key removed.
- c. The MDC will not be stored in any location that exposes the MDC to extreme heat or cold.
- d. Employees will initiate a session lock (activate password protected screen saver) on the MDC if it is to be left unattended. This can be accomplished by pressing the windows menu key and letter "L" on the keyboard or by pressing Ctrl+Alt+Delete and selecting "Lock this Computer." Unattended means anytime the MDC is outside your immediate view or control.

5. Stolen Vehicles and/or MDC
 - a. The Bureau Commander, Bureau of Criminal Investigations and Intelligence will be notified immediately if it is believed that an MDC (or a vehicle with an MDC in it) is stolen.
 - b. Employees assigned MDC equipment will be held responsible for any stolen or missing item if the vehicle is left unlocked when unattended.
 - c. Stolen equipment requires the completion, and submission through channels, of an appropriate UCR report (sworn members) or completion of a memorandum detailing the particulars of the loss (non-sworn personnel).
6. Employees will not give their passwords to any other persons to use nor will they leave the password in any discernible written form on or near the MDC.

B. RESTRICTIONS REGARDING ACCESS TO CRIMINAL JUSTICE SYSTEMS

Systems include, but are not limited to: FCIC, D.A.V.I.D, LiNX and other Confidential Law Enforcement Data Information Systems.

1. Employees **will**:
 - a. Restrict dissemination of information received through Confidential Data Systems to authorized criminal justice persons only.

MDC users are responsible for maintaining a Criminal History Dissemination Log (HSMV 61042) if disseminating criminal history outside of FHP.
 - b. Perform transactions for criminal justice purposes only.
2. Employees **will not**:
 - a. Access criminal history files except as provided for by law and rule.
 - b. Access database records for any reason other than legitimate law enforcement purposes.
 - c. Permit use of the MDC by any individual who is not certified for Confidential Law Enforcement Data Information Systems access.

C. AUTHORIZED/UNAUTHORIZED USE

1. Use of the MDC is restricted to official FHP business. Computer files, including e-mail messaging and FCIC inquiries are subject to review.
2. Use of the MDC by anyone other than authorized Division employees requires authorization from the Troop Commander in consultation with the Chief Technology Officer.

3. Employees are responsible for ensuring the security of the MDC against unauthorized use.
4. If it is believed that unauthorized access has occurred, the employee will immediately notify a supervisor.
5. Inappropriate or unauthorized use of the MDC may subject the employee to disciplinary action.
6. Unless exigent circumstances arise, all members assigned or sharing a MDC or desktop computer shall, at least twice during their assigned shift, read and, if required, respond to any email correspondence sent to their assigned account. Checks shall be timed close to the start and the end of the shift. Also, members shall abide by any orders or instructions they receive via email from a superior member.

D. SOFTWARE RESTRICTIONS

1. DHSMV Policy #8.01, Computer Security, regarding department computers and software is applicable to MDCs.
2. If an employee wants additional software loaded onto the MDC, they must submit a written request through the chain of command to the Troop Commander. If the Troop Commander determines that the additional software is appropriate, he or she will forward the request to Chief Technology Officer. Only software that is business related will be approved. Screen savers, wallpapers, games and other non-business-related software are not to be loaded onto MDC (this does not include software contained on the MDC at the time of purchase).
3. Any unauthorized and/or altered software found on FHP MDCs during maintenance work, upgrades or inspections will be removed and the employee may be subject to disciplinary action.

THE MANIPULATION OR ALTERATION OF CURRENT SOFTWARE RUNNING ON-AGENCY OWNED MOBILE, DESKTOP OR HANDHELD COMPUTERS IS PROHIBITED.

4. Employees will not disable or shut off any anti-virus or anti-spyware programs.

E. MDC OPERATIONS

1. Unless specifically exempted by the Director, the user will be logged into the SmartMCT Mobile Application on their MDC at all times the member is on duty. This does not apply to members traveling out of state or who cannot receive a signal due to assignment (aircraft operations).
2. Members will take care when operating an MDC while driving. Simple inquiries and viewing the nature of an in-coming message may be performed while driving. Message response and complex or multiple inquiries are not to be conducted while driving.

3. Foods and beverages are not to be placed on the MDC unit. Care is to be taken to ensure no food, beverage, or other substances are dropped or spilled on any part of the MDC unit.
4. Only members with current FCIC certification are permitted to initiate inquiries into criminal justice databases.
5. Members will not use any other member's login name and/or password to log onto an MDC unit.
6. At all times when MDC usage is required by this policy, the Automatic Vehicle Locator (AVL) function of the SmartMCT application on the MDC shall be used if the MDC is equipped with a Global Positioning Satellite (GPS) unit or configured to interface with an in-vehicle GPS function (i.e. GPS-equipped mobile router).
 - a. No member shall change any settings or configurations of the MDC software, or make any physical changes to the MDC to cause the GPS to fail to properly report location information to the CAD system.
 - b. If a vehicle is equipped with an in-car mobile router, members shall ensure the USB modem ("beam") and mobile data SIM card are installed and transmitting any time the vehicle is in operation. If the member determines the modem is not operating properly, he or she must notify a supervisor immediately and contact TAC for resolution. If resolution is not immediately available, the member may connect the USB modem directly to his or her MDT until the router can be replaced or repaired. In all cases, these actions must be reported to the member's supervisor and documented by contacting TAC. The member should make every effort to have the router repaired as soon as reasonably possible.

Members are authorized to connect the USB modem directly to their MDT when the vehicle is not in motion, mobile data is necessary for them to perform work functions, and other data sources are not available. In such cases, the modem must be returned to the mobile router prior to resuming operation of the vehicle.
 - c. If the MDC fails to properly report location information to the CAD system, the member shall immediately notify their supervisor, or his/her designee, and TAC of the failure so that appropriate repairs can be made to restore the AVL function. TAC will not need to be notified during short periods of lost connectivity.
7. If a member's assignment would be adversely affected by having location information published in the CAD system, the member's Troop Commander, or someone of equivalent rank, may authorize the CAD administrator or the Chief Technology Officer to disable the display of location information in the CAD system for as long as necessary to

complete the assignment. At the conclusion of the assignment, the AVL function shall be promptly activated to normal operations.