CHAPTER 26

MOBILE DATA TERMINALS (MDT) 04/07/10

Policy

It is the policy of the Cecil County Sheriff’s Office to ensure proper operation of the Mobile Data Terminal (MDT) and that the MDT’s are being utilized securely and confidentially.

Purpose

The Cecil County Sheriff’s Office will use wireless communication technologies to enhance the operations and security of the Agency. Employees will use the Mobile Data Terminals (MDT) in compliance with the policies and procedures outlined.

A. General MDT System Usage

1. The Dispatch Manager is responsible for the agency’s management and operations of the MDT Program as well as communication and interaction between Federal, State and local agencies that support the MDT Program.

2. The Cecil County Sheriff’s Office Information Technology Department (IT) will be responsible for the daily administration of the MDT Program as well as maintenance and repair. Additionally IT will conduct random administrative security checks of the MDT system to ensure that all necessary security procedures are being followed.

3. It is the responsibility of each Deputy Sheriff to ensure this technology is only used for conducting authorized agency business and in a manner that does not compromise confidential, protected, restricted or other sensitive information.

4. MDT users will report, by the end of their shift, all MDT related issues or problems to their supervisor who will document the issue or problem and forward that information to the IT department for review and/or solution.

5. If the equipment needs to be serviced, repaired or reprogrammed, a message will be sent to the IT department.

B. System Security

It is the assigned deputy sheriff’s responsibility to ensure the security of the MDT against unauthorized use.

1. Password- The password used to access the MDT system and METERS/NCIC will not be shared or made known to any other individual, nor will the Deputy Sheriffs leave their password in any discernible written form on or near their computer. Deputy Sheriffs will be held strictly accountable for any transactions appearing under their log on signature and password. Deputy Sheriffs, however, may be required to disclose this information to someone in their chain of command for CCSO business purposes.

   Deputy Sheriffs who have reason to believe their password has been compromised will immediately notify their supervisor and the IT department and change their password. An attempt by any employee to utilize an MDT or gain access to METERS/NCIC with another employee's password is strictly prohibited.

2. Vehicle Security- It is the assigned Deputy Sheriff's responsibility to safeguard the MDT. The MDT's will be securely locked into place on the docking station while the computer is in the vehicle. Deputy Sheriffs will lock their vehicle upon exiting. All Deputy Sheriffs are required to log off from all network computer systems at the completion of their workday.

3. Transporting Prisoners- Special care must be taken to safeguard information when transporting prisoners. The deputy sheriff will lock the system or close the laptop cover during prisoner transports.

C. Prohibited Uses

1. MDT's contain sensitive law enforcement information. Use of or access to the MDT's by unauthorized persons is prohibited.

2. The unauthorized introduction of software programs or other files or, the manipulation or alteration of current software running on agency owned mobile, desk top or handheld computers is strictly prohibited.

3. All MDT's, data and software, maintained or used by the Cecil County Sheriff's Office is for official use only. Deputy Sheriffs will not use or cause to be used any MDT for personal gain or benefit of any kind.

4. Deputy Sheriffs will not attempt to install, delete, or modify any software or hardware associated with the MDT at any time.

5. Deputy Sheriffs may not access information concerning individuals who are not subject to legitimate police inquires.

6. Violations of prohibitions may result in disciplinary action or criminal

prosecution.

D. Mobile Data Browser General Procedures

1. MDT usage is restricted to those Deputy Sheriffs trained in the proper use of the equipment and granted access into the system. All MDT operations will be in accordance with Internet Explorer 8 standard agency operating procedures.

2. Deputy Sheriffs will turn on and log into the MDT system at all times (on and off duty) while operating their agency vehicle. The MDT will remain on at all times the Deputy Sheriff is on or off duty. Deputy Sheriffs will not operate **any** mobile laptop computer while their vehicle is in motion. Deputy Sheriffs assigned MDT's will stop their vehicle and park in a safe manner before attempting to access information.

3. When the MDT system is not in use, the laptop cover will be closed or covered.

4. MDT users will attend all scheduled MDT related training. Should a conflict exist between scheduled training and another assignment, the MDT user will inform his/her supervisor of the conflict. The supervisor will attempt to resolve the conflict or arrange for the Deputy Sheriffs training to be rescheduled for the next available training date.

5. Safe operation of the patrol car is paramount. It is stressed that common sense and safe driving practices dictate the Deputy Sheriff will focus his/her attention on safe operation of the vehicle and view the MDT only when it is safe to do so. MDT devices will only be operated when the vehicle is **not** in motion.

E. CJIS/NCIC/METERS Information Systems

1. CJIS/NCIC/METERS will be accessed via the MDT's, by the authorized users. These systems offer detailed information concerning the personal and physical identity of individuals which may be of concern to law enforcement.

2. Maryland law prohibits secondary dissemination of CJIS information for other than official purposes. This information applies to motor vehicle and licensing information obtained through CJIS. Any person disseminating

criminal justice information to unauthorized recipients is subject to Federal and State imposed sanctions.

3. Only Deputy Sheriffs who have been trained to access METERS (Maryland Telecommunications Enforcement Resources System), NCIC (National Crime Information Center), and CJIS (Criminal Justice Information System) may use the entry into those records and motor vehicle information files.

4. Deputy Sheriffs are required to use the MDT's to make all CJIS/NCIC/METERS inquiries unless circumstances exist, that makes using the MDT impractical, or endangers officer safety.

5. Responses from inquiries to CJIS/NCIC/METERS are protected information. Deputy Sheriffs are not permitted to use these systems for their own use or purposes. Information received through these computer systems may only be used for official criminal justice purposes. Deputy Sheriffs will not initiate any inquiry outside those purposes necessary to complete a law enforcement or agency objective.

6. Deputy Sheriffs will ensure that unauthorized persons, to include passengers or offenders located in the vehicle, do not view responses from these systems. When the MDT system is not in use, the laptop cover will be closed or covered.

7. Deputy Sheriffs are responsible for maintaining all certifications, which allow access to CJIS/NCIC/METERS, and other databases retrievable by an MDT.

F. Warrant and Stolen Property Verification

1. Special care must be taken in using the MDT to check warrants. Not all local warrants have been entered into the system. The absence of a warrant in the system does not necessarily mean there are no local warrants. The Deputy Sheriff must still have dispatch confirm the status of an active warrant.

2. The Deputy Sheriff will also confirm with dispatch, all hits received as a result of an NCIC query with regards to stolen property

3. Warrant or stolen property information received from the MDT will **not** be considered probable cause for arrest. Warrant and stolen property hit confirmation procedures include:

(a) Deputy Sheriffs receiving a hit on his/her MDT, will verify the hit by viewing the NCIC summary screen to ensure the HIT applies to the person or type of property which has been queried, and that the information they requested matches the query results provided by the system. The Deputy Sheriff should follow this procedure prior to initiating a stop, contact or other law enforcement activity when ever possible unless, other probable cause exists for the stop.

(b) Deputy Sheriffs must confirm a warrant or stolen property hit through dispatch prior to making an arrest or recovery. Waiting for the hit confirmation, does not prohibit the deputy sheriff from taking the necessary precautions to secure the suspect individual for officer safety.

G. Care of Equipment

1. Care must be taken when handling all MDT Devices. Avoid exposing the laptop unit to moisture, including rain and snow, as well as beverages. If spillage does occur, log off all active sessions and shut down the MDT immediately. Clean the affected area, and notify the IT Department. Do not power-on the MDT Device until such time as the IT Department has had an opportunity to inspect the device.

2. The MDT is capable of operating in diverse weather however; it may not function properly until it returns to ideal operating range. In the extreme cold, the device may not function until the device heats up. In the extreme heat of summer, the device may not work until the ambient temperature of the vehicle had cooled down.

3. Care should be used in cleaning the screen of the MDT. An anti-static cleaning cloth should be used to clean the screen. Another cleaning method may be the use of a soft cotton cloth lightly moistened with water. No cleaning solution of any kind should be used to clean the screen or laptop device. No cleaners of any type such as Windex will be used on the screen.

4. For those MDT’s having a touch screen, users will only use a “fingertip” when touching the screen. Under no circumstances will an ink pen be used on the screen. The ink pen can cause irreparable damage to the screen.

5 Any maintenance or repairs that need to be done to the MDT’s will be done exclusively through the IT Department, as well as any adjustments that are needed.

6. The MDT will be removed from the vehicle at the end of the users tour of duty as well as when the vehicle will be left unattended for any extended

period of time, to include routine vehicle maintenance or left at another repair facility.

H. Safety and Inspections

1. MDT's will undergo monthly inspections by Supervisory Personnel. This information will be documented in the Vehicle Inventory/Inspection Form/CCSO Form SO-027, and if any deficiencies are noted, the IT Department will be notified promptly.

2. For officer safety, the MDT should always be properly secured in the vehicle mount, and in-line with the center console so it does not interfere or impede with the operation of the passenger side air bag.

3. Wireless mobile computing devices may interfere with the function of inadequately protected medical devices including pacemakers.

4. Wireless mobile computing device users will be mindful of regulations governing the use of the device. The user will deactivate the device in areas where radio devices are forbidden, or when it may cause interference or danger. Any restrictions on use pertaining to cell phones and two-way radios will apply to the MDT's. Similar to radio transmission, special attention should be used in the following areas: fuel depots, chemical plants, blasting operations, and all other areas where radio transmissions are either prohibited or restricted.