MOBILE DATA TERMINALS

WRITTEN DIRECTIVE: 1.15
EFFECTIVE DATE: 04-01-2011
REVISION DATE: 05-30-2016

Contents

I. Purpose

It is the purpose of this Written Directive to provide members with guidance on the proper use of Mobile Data Terminals.

II. Policy

The availability and use of the Mobile Data Terminal within the work environment provides many opportunities for enhancement of productivity and effectiveness. This technology also provides the opportunity for rapid transfer and broad distribution of sensitive information that can also have damaging effects on this agency, its members and the public if not managed properly. Therefore, it shall be the policy of the University of Maryland, Baltimore Police Force (UMBPF) that all members abide by the guidelines set forth herein when using the Mobile Data Terminal (MDT).

III. Background

The Mobile Data Terminals serve as a conduit for several systems. The Capital Wireless Information Net (*CAPWIN*) is a regional network of public safety and transportation agencies in Maryland, Virginia and the District of Columbia. The mission is to enable and promote interoperable data communications, operational data access and incident coordination and situational awareness across jurisdictions. The DELTA + system is Maryland based and allows officers to electronically complete and submit accident reports, warning citation, moving citations, and provides MVA and criminal information based on an officers level of access. The MDT also provide mobile access to the Automated Records Management System (ARMS)

IV. Definitions

A. Mobile Data Terminals (MDT)

For the purpose of this Written Directive, MDTs are protable computer terminals, often mounted in the police vehicle, capable of accessing electronic mail systems, electronic bulletin boards, Internet services, METERS, Automated Records Management System (ARMS), Delta Plus, and other law enforcement programming.

B. Systems Administrator

The LAN Administrative Manager refers to the manager of acquisitions, installation, configuration, hardware, maintenance and repair of all equipment associated with the MDT program.

C. Program Manager

The manager of the MDT programming for the UMBPF will be assigned by the Associate Vice President for Public Safety and shall be responsible for the day-to-day operations of the various systems with the exception of training, installation, configuration, maintenance, hardware, repair and acquisitions.

D. Training Coordinator

All training on the MDT will be coordinated by the Education and Training Section in cooperation and consultation with the Communications Center and Records Section of the UMBPF.

E. Approved Terminal Software

Approved software includes only legally licensed software authorized by the LAN Administrative Manager for use on a UMBPF workstation or a specific computer server.

F. CAPWIN Authorization

CAPWIN programming is authorized by the University of Maryland (College Park) Department of Civil and Environmental Engineering's Center for Advanced Transportation Technology. It operates under the guidance of a Board of Directors made up of representatives from local, state and federal first responder agencies. Mobile clients are designed for maximum performance in wireless, field environments and permit local queuing, messaging and local rendering of GIS maps using network linking.

G. Media

Audio and visual media used for the creative convergence of arts, science and technology for social interaction and education.

H. E-TIX Coordination

The Maryland Electronic Traffic Exchange Program (E-TIX), a module of Delta Plus, was developed to assist law enforcement with the safe and timely means of issuing traffic citations by providing the software to scan bar codes on a driver's license.

I. ACRS Coordinator

The Automated Crash Reporting System (ACRS), a module of Delta Plus, was developed to assist law enforcement in preparing and submitting accident reports and investigations in an electronic format to the Maryland State Police.

J. METERS

The Maryland Electronic Telecommunication Enforcement Resource System (METERS) refers to the switching system managed by the Maryland State Police giving access to in-state and out-of -state wanted data. The system also combines the functions of the National Crime Information System (NCIC) and the Criminal Justice Information System.

V. Authority

A. Program Manager Responsibilities

The Program Manager is responsible for the daily administration of the UMBPF MDT program. Program management is assigned to _____ (what position)

B. Supervisors

Supervisors are responsible for the monthly inspection of all equipment. Damage, possible software alterations and problems with functionality will be reported to the LAN Administrative Manager immediately.

C. User Requirements

1. Members are required to maintain all certifications that allow access to METERS. Only those members who have been certified may use the system.

2. Passwords shall not be shared or made known to any other individual.

3. Members who have reason to believe that their password has been compromised shall immediately notify the Education & Training and IT Sections.

4. Attempts to gain access to any password protected system with another member's password are strictly prohibited. MDT computers shall only be used for official business purposes consistent with other provisions of this Written Directive.

VI. Using the MDT

A. Computer Use/Application and Privacy

1. The following rules apply to all media accessed on or from the MDT.

    a. Transmission of electronic messages and information on MDTs provided for employees of the UMBPF shall be treated with the same degree of propriety, professionalism and confidentiality as official written correspondence or verbal communication.

    b. This agency encourages authorized and trained personnel with access to a MDT to utilize these devices whenever necessary. However, use of any of these devices is a privilege that is subject to revocation.

    c. Any correspondence sent or received using the CAPWIN program may be retrieved by authorized personnel, even though the transmission may have been deleted. Information sent or retrieved using the MDT can be subject to review in an administrative, internal, civil or criminal case.

2. Privacy

    a. MDTs and their programs are the property of the UMBPF and intended for use in conducting official business with limited exceptions noted elsewhere in this Written Directive.

    b. Members are advised that they do not maintain any right to privacy when using equipment belonging to the UMBPF.

    c. As a result, the LAN Administrative Manager may monitor any information placed on or extracted from an MDT.

    d. The LAN Administrative Manager may also access, for quality control purposes or for violations of this Written Directive, any electronic transmissions of members conducting the business of this agency.

B. Prohibitions

1. Accessing or transmitting materials that involves the use of obscene language, images, jokes, sexually explicit materials, or messages that disparage any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material.

2. Confidential, proprietary, or sensitive information may be disseminated (or made available through shared directories or network systems) only to individuals with a need and right to know and when there is sufficient assurance that appropriate security of such information will be maintained. Such information includes for example:

    a. Transmittal of personnel information such as salary, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records, or related employee information; and

    b. Criminal history information and confidential informant master files, identification files, or related information.

3. No e-mail or other electronic communications may be sent that attempts to hide the identity of the sender or represents the sender as someone else.

4. Media may not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other members to access and use the system.

5. Members may not copy, retrieve, modify, or forward copyrighted materials except as permitted by the copyright owner or except for a single copy for reference use only.

6. No member shall access or allow others to access any file or database unless that person has a need and a right to such information.

7. An MDT is designed and intended to conduct the business of the UMBPF and is restricted to that purpose.

8. Off-duty personnel may make use of MDTs for professional and career development purposes when in keeping with other provisions of this Written Directive and with prior knowledge of an appropriate supervisor.

9. With supervisory approval, a member may use the MDT while on special assignment outside of the jurisdiction of the UMBPF.

10. Employees may not attempt to read or "hack" into other systems or logins; "crack" passwords, breach computer or network security measures, or monitor electronic filings or communications of other employees.

11. Changing any of the program settings in any system other than those expressly permitted in this Written Directive is not authorized.

C. Personalizing the MDT

1. While operating the MDT, users may personalize the MDT for day/night viewing, location, unit and contact telephone numbers, messaging alerts and docking privileges.

2. Passwords can be changed as long as they contain 8-14 characters (case sensitive) and contain 2 numbers and 2 letters.

D. CAPWIN

Users may join the on-line communication regarding a specific incident by clicking the "Join" button on the Incident Information Pane in CAPWIN. If the "Join" button does not appear, you are already a part of the incident.

1. Queries in CAPWIN

a. Logging-on to the CAPWIN system does not give the user access to the NCIC database. Separate user identifications as well as passwords will be issued for this purpose.

b. Queries can be made by using personal identifiers such as name, date of birth, sex, race and state. All "hits" on the CAPWIN system, however, must be confirmed.

c. Results from a query will list aliases, social security numbers and dates of birth.

d. If the results of queries are highlighted in the color *Red*, a warrant or caution has been issued.

2. On-Line Help for CAPWIN

Live on-line help can be accessed in an instant message format from the CAPWIN Help Desk.

3. Establishing "Contacts"

Members can add other CAPWIN users to their "My Contacts" list for quick access to phone numbers and instant messaging.

4.. Establishing "Chat Rooms"

a. Members may establish Chat Rooms or participate in other Chat Rooms with CAPWIN personnel from this agency or other agencies. Although private and public Chat Rooms are available on the system, only participation in *public* Chat Rooms will be permitted by UMBPF personnel.

b. Members participating in a Chat Room shall conduct themselves appropriately keeping in mind that all information made a part of the CAPWIN system is memorialized and can be recreated even when the information has been deleted.

E. ARMS Mobile

1. ARMS Mobile consists for two systems; Mobile Report Writer (MRW) and Mobile Computer Aided Dispatch (MCAD)

    a. MRW allows authorized persons to create and electronically submit police reports.

    b. MCAD allows authorized users to create their own CAD events while on patrol.

2. ARMS Mobile is a password protected system

    a. Access to the system is provided by the System Administer

    b. Password updates by the user is required to maintain access to the system

3. Training on the system is coordinated through the Education and Training Unit and facilitated by the Records Section.

F. Delta Plus

1. The Delta Plus (Delta +) system has several modules', E-Tix and ACRS

    a. The Maryland Electronic Information Exchange Program (E-TIX) was developed to assist Maryland law enforcement with a timely means of issuing traffic citations and accumulating pertinent related data. The program is a vehicle-based computer scanning system that permits the scanning of the bar code on the driver's license for the purpose of writing a moving citation or warning citation. Commensurate with printing the citation, the data is also scanned through a number of databases within the CAPWIN system for wanted checks, license and vehicle suspensions, etc. After scanning the license, a copy of the citation can be printed and issued to the violator. Subsequently, court dockets are sent to the issuer that can be used to testify in court.

b. The ACRS module, similar to E-Tix, is a vehicle-based computer system that allows officers to enter and record accident information and investigations. The reports are submitted electronically to the Maryland State Police.

2. The Maryland State Police has complete authority to regulate the DELTA + system, including establishing rules and regulations, providing program management data analysis and training.

3. Each participant will adhere to all requirements of the E-TIX program to remain certified. If certifications are suspended or revoked for any reason, the participant will require refresher training before certification can be reestablished.

VII. Software and Electronic Mail

A. External Source Downloading

1. Members shall not download or install on their MDT any file, software program or other materials from the internet or other external sources without the express permission of the LAN Administrative Manager.

2. The manipulation or alteration of software, hardware, peripheral devices, screen savers, or other attachments running on MDTs without the permission of the LAN Administrative Manager is also prohibited.

3. Members shall observe copyright and licensing restrictions for all software.

4. Any software found on an MDT that has been placed there in violation of this Written Directive shall be subject to removal by the LAN Administrative Manager.

5. Members shall also observe copyright restrictions of any documents, images, or sounds sent through or stored on electronic mail.

6. Any hardware enhancements or additions to agency-owned equipment must be approved and authorized by the LAN Administrative Manager. The LAN Administrative Manager is responsible for determining proper installation procedures.

B. Unauthorized System Use

To avoid breaches of security and to avoid overloading the system, members shall log-off their assigned MDT whenever they are not actively engaged in UMBPF business. The CAPWIN system will automatically close after 8 hours.

VIII. Vehicle Operations

A. Safe Operation

The safe operation of a police vehicle shall always be the driver's primary responsibility. As such, the use of the MDT shall be limited when the vehicle is in motion and must not impair the operator's ability to drive in a safe manner. Members shall consider the need to safely stop the vehicle before using the computer. The use of the MDT will always be secondary to the safe operation of the vehicle.

B. Securing the Terminal

The MDT must be locked in the docking station and properly secured at all times while in use.

C. Calls for Service

Calls for service will be communicated both verbally and using the wireless connection to the mobile terminal. All calls for service will continue to be dispatched verbally so that supervisors and back-up units can be apprised of all events occurring on campus.

D. Terminal Repairs

Repairs shall be made or coordinated by the LAN Administrative Manager. As soon as possible after discovery and never later than the end of their shift, members shall report all damage and/or technical problems to their immediate supervisor (including damage caused by traffic accidents) and memorialize the information in a police report or on an Administrative 95 Form as required by a supervisor.

E. Vehicle Maintenance

When UMBPF vehicles are out of service for vehicle maintenance, the MDT will be removed and retained by the officer until the vehicle is repaired. Should repair of the vehicle span shifts, the terminal will be returned to its storage location. The user will be responsible for the security of the terminal while assigned to a particular police vehicle.

Antonio Williams, MS
Chief of Police / Associate Vice President for Public Safety