SPRINGFIELD POLICE DEPARTMENT

Standard Operating Guideline

Effective Date: 12/31/2013	Supersedes Policy Dated: 11/30/2012	Rescinds:	SOG Number: 308.4
Accreditation Index:			
Part Title: Support Services	**Chapter Title:** Informations Systems Management		
Chief of Police:			

Mobile Data Communications System

I Policy

The purpose of the Mobile Data Communication System (MDCS) shall be to improve the City of Springfield's public safety responsiveness by utilizing data communications in police vehicles. It is the policy of the Springfield Police Department that all personnel shall adhere to department training and the provisions herein regarding the use of the Mobile Data Communications System.

II Definitions

Assigned Employee - A police department employee who has been assigned a department Mobile Data Terminal.

Hardware –Equipment that makes a computer system, e.g. monitors, printers, or peripheral equipment etc, as opposed to the software used on it.

Log On (Sign On) - A process that the assigned employee performs to open a computer program or system, may also refer to a name and password or other appropriate commands used for logging on to a computer.

Log Off (Sign Off) - A process that the assigned employee performs to close a computer program or leave a computer system.

MDT Communications – Includes Talk, Announce and Mail used for sending electronic messages from one person to another person or group of individuals via use of Mobile Data Terminal.

Mobile Data Terminal (MDT) – Computers having access to the Mobile Data Communications System.

Network - A system of interconnected computers which allows the sharing of files, software, printers, or peripheral equipment.

Software - Computer programs and applications ran on a computer system, e.g. word processing or database packages.

System Administrator - The Information Systems (IS) Network Technician assigned to the Police Department responsible for the operation and maintenance of the Mobile Data Communications System.

System Maintenance and Installations – Additions, modifications or deletions of any software or hardware to the Mobile Data Communications System.

Unauthorized Software - Any software that has not been approved

III Procedure [1]

1 The Mobile Data Communication System was designed to allow access to various federal, state and local databases and provides a secure method of communication between field units.

1.1 Computerized networks include but are not limited to the Missouri Uniform Law Enforcement System (MULES), Springfield-Greene County Computer Aided Dispatch (CAD), City, Police Department networks, and Police Records Management System (RMS).

1.1.1 The Mobile Data Terminals, hardware, software and other equipment referred to under this guideline relate only to the Mobile Data Communication System unless otherwise specified.

2 The Mobile Data Communication System is for work related activity, personal use of information or equipment is strictly prohibited.

3 No employee will attempt to gain access to any area they are not authorized.

3.1 This includes, but is not limited to:

3.1.1 Other employee MDT communications;

3.1.2 File folders; or

3.1.3 Hard drives.

1 III Procedure, grammatical correction, per Policy Change Order 13-122, Effective Date 12/31/2013.

4 The assigned employee is responsible to physically safeguard the MDT from theft, destruction or unauthorized use. (i.e. locking their vehicles when left unattended.)

4.1 ALL information is considered to be confidential and shall not be disseminated to the general public.

4.2 Employees shall secure the screen display so that it cannot be viewed by unauthorized persons.

4.2.1 Close the lid on laptop computers when not in active use.

4.2.2 If the assigned employee leaves the MDT unattended they should lock their Windows session by selecting Ctrl+Alt+Delete, Lock Computer.

4.3 Employees will not give their passwords to any other persons nor will they leave the password in a discernable written form in or near their computer.

4.3.1 Employees may be required to disclose this information to chain of command or support personnel for department business purposes.

5 Mobile Data Communications System training is conducted during the Police Academy and updated periodically during In-Service Training as necessary.

6 Mobile Data Terminals

6.1 MDTs are used to obtain information from various law enforcement databases.

6.2 MDTs require a user to log on to gain access to the system.

6.3 Use of a MDT by anyone other than authorized department employees requires authorization from the employee's supervisor.

6.4 MDTs may be operated while the vehicle is in motion

6.4.1 The driver of the vehicle shall remain cognizant of traffic conditions while exercising normal care, safe operating practices, and considering the hazards of operating any other device such as the MDT, cell phones, two-way radios, etc.

6.5 Mobile Cop

6.5.1 Mobile Cop is an application within MDCS that gives the user access to the Missouri Uniform Law Enforcement System (MULES) and the Springfield-Greene County Computer Aided Dispatch (CAD) system and requires the user to log on the system for access.

6.5.2 MULES

6.5.2(a) Missouri State Highway Patrol MULES certification course must be completed prior to access.

6.5.2(a.1) It is the responsibility of the assigned employee to maintain MULES certification.

6.5.3 CAD

6.5.3(a) Officers will perform the following functions in CAD when time and safety allows:

6.5.3(a.1) Check pending and active calls for service.

6.5.3(a.2) Obtain Case Numbers.

6.5.3(a.3) Initiate the following incidents:

6.5.3(a.3.1) Breaks

6.5.3(a.3.2) Service Center / Maintenance

6.5.3(a.3.3) Car Wash

6.5.3(a.3.4) Admin Time: Court, HQ, SDS, or Reports – These shall have events logged and are not status changes.

6.5.3(a.3.5) Directed Enforcement – Traffic Officers Only

6.5.3(a.3.6) These are the only call types officers are authorized to initiate themselves, all other call types are initiated by the Springfield/Greene County Emergency Communications Department.

6.5.3(a.4) Change Call Status – with the exception of emergency response to life-threatening incidents and other situations where officer safety becomes an issue during arrival, officers are responsible for showing themselves in route, arrived and cleared from all calls dispatched via the MDT.

6.5.3(a.4.1) The status change shall also be broadcast verbally via the radio.

6.5.3(a.5) The primary unit is responsible for disposition of all calls.

6.5.3(a.5.1) HBO, GOA or UNF calls require a short written explanation in the comments section of the justification for the HBO, GOA or UNF classification.

6.6 MDT Communications

6.6.1 Messages sent on the MDT Communications system will be for departmental business.

6.6.2 An employee shall not attempt to gain access to another employee's communications.

6.6.3 Employees shall make their mail available to a supervisor in their chain of command upon request.

6.6.4 Communications sent through the Mobile Data Computer System may be retrieved by authorized personnel at a later time, even though it may have been deleted from the assigned employee's account.

6.6.5 MDT Communications may not be protected under the Missouri Sunshine Law and could be subject to a discovery motion in a criminal case, civil case, or internal investigation.

6.6.6 Communications should be considered in the public domain. Messages should be professional and courteous.

7 SYSTEM MAINTENANCE

7.1 The System Administrator is responsible for all maintenance, support and repair of the equipment related to the Mobile Data Communications System.

7.2 No software or hardware will be loaded or installed on the Mobile Data Communications System without authorization.

7.3 Personal computers or other equipment may not be connected to the Mobile Data Communications System without authorization.

7.4 The following procedures should be followed to receive authorization for new software and equipment:

7.4.1 A written request shall be submitted, through the Chain of Command, approved by the Chief of Police or Bureau Commander and Information Systems.

7.4.1(a) The written request should contain the following information:

7.4.1(a.1) A needs analysis;

7.4.1(a.2) A statement of how the equipment will benefit the department; and

7.4.1(a.3) The training requirements if the equipment is approved.

7.4.1(b) If the request is approved, a copy of this approval should be forwarded and processed in accordance with current department policy regarding purchases.

7.4.1(c) If the request is denied, the reasons will be provided to the requesting officer by the System Administrator.

7.5 The System Administrator should be notified via email as soon as possible if equipment within the mobile data system malfunctions, is damaged, stolen, or it is believed unauthorized access was attempted or gained.

7.5.1 The following information should be documented:

7.5.1(a) Date and time of occurrence;

7.5.1(b) Detailed description of the problem;

7.5.1(c) Vehicle experiencing the problem;

7.5.1(d) If the problem be re-created;

7.5.1(e) Reporting person and contact telephone number.

8 USER ACCOUNT MAINTENANCE AND INSPECTIONS

8.1 New employees needing mobile data access accounts should notify their supervisor of this need.

8.1.1 The employees direct supervisor should make a request through the chain of command for account approval via email.

8.1.1(a) Final approval should be forwarded to the System Administrator via email.

8.2 Personnel leaving employment with the Springfield Police Department will have their mobile data access accounts deleted.

8.2.1 It is the employee's direct supervisor's responsibility to notify the System Administrator via email when an employee is no longer employed by the SPD.

8.2.1(a) The Support Operations Section Commander will ensure that the System Administrator conducts an audit of users every 90 days to determine the accuracy of user accounts. The Commander will provide proper documentation of the results through an IDC. [2]

8.3 The MDCS computers are subject to line or staff inspections at any time.

9 LOG FILE ACCESS

2 Section 8.2.1(a) revised mobile data account audit process, per Policy Change Order 13-122, Effective Date 12/31/2013.

9.1 The System Administrator and all Internal Affairs Investigators can access and search the log files created by the Mobile Data Communications System.

9.2 Users of the system can see their own log files, but not those of other users.

9.2.1 Requests to see log files of others must be approved by a lieutenant or above.

9.2.2 Requests for access shall be forwarded to the System Administrator via Email.

9.3 The System Administrator may release log file information to Springfield-Greene County E911 upon request.

9.3.1 Other requests from outside agencies must be approved by a lieutenant or above and may require a subpoena for release.

9.4 Log files will be retained for a period of 2 years in accordance with the Record Retention schedule as published by the Missouri Secretary of State.

IV Attachments