


# TEXARKANA POLICE DEPARTMENT

## GENERAL ORDERS MANUAL

<b>SUBJECT</b>	<b>Mobile Data Computers</b>		
<b>NUMBER</b>	<b>1109.02</b>	<b>EFFECTIVE DATE</b>	<b>March 18, 2011</b>
<b>Scheduled Review Date</b>	<b>March 01, 2017</b>	<b>ISSUE DATE</b>	<b>March 18, 2011</b>
<b>DATE REVIEWED</b>		<b>REVISION DATE</b>	<b>March 12, 2015</b>
<b>APPROVED BY</b>		<b>(Reserved for Expansion)</b>	

### I. Scope and Purpose

- A. The purpose of this policy is to define the guidelines for the proper operation of the Texarkana Police Department's Mobile Data Computer (MDC) system.
- B. The Mobile Data Computer system is intended to enhance the officer's ability while in the field to obtain necessary computerized information in a timely manner, reduce radio traffic, provide computer aided dispatch information, provide access to the PMAM HCM training module, and to increase officer safety.
- C. The Mobile Data System is not designed, nor is it intended, to replace voice communications transmissions.

### II. Policy

- A. It shall be the policy of the Texarkana Police Department to authorize the use of Mobile Data Computers, and that the use of these computers will be accomplished in a lawful, safe, and effective manner.

### III. Definitions

- A. **Mobile Data Computer:** Any laptop or portable computer issued for the purpose of field reporting, data collection or any other field use.
- B. **Field Use:** Any use of a mobile data computer connected to a computer system housed in the Texarkana Police Department via wireless equipment.
- C. **User:** Any person utilizing any Texarkana Police Department computer system or network for the purpose of information exchange, storage or reporting.

### IV. Procedures

- A. All transmissions of data and/or queries via the Mobile Data Computer (MDC) system are limited to official Texarkana Police Department business pertinent to a legitimate and lawful law enforcement functions.
- B. The content of all transmissions over the MDC system shall comply with the same requirements as with voice radio transmissions, which are governed by the FCC and Texarkana Police Department

Page 1 of 3    Number: 1109.02	Effective Date: March 18, 2011
Subject: Mobile Data Computers	<b>Revision Date: March 12, 2015</b>

policies and procedures. Additionally, MDC transmissions shall comply with the requirements described in the Texarkana Police Department's Email and Computer Use Policy. For additional information regarding these requirements, refer to [General Order 1109.01---Use of Computer Equipment, Email and Internet Access](#).

- C. Obscene, derogatory, racial, demeaning, or sexual remarks shall not be transmitted.
- D. The MDC shall not be used to conduct personal business for any reason.
- E. Communications and other information accessible by this device are not intended for distribution to the general public.
- F. All MDC messages are recorded and retained as official records of the Texarkana Police Department. As such, they are subject to release pursuant to a Freedom of Information request. For more information regarding FOI requests, please refer to [General Order 1102.16---Freedom of Information Requests](#).
- G. Inappropriate use of the MDC system is prohibited. To ensure compliance with this policy, the Chief of Police has developed a system by which the computer activity of a random selection of department personnel is examined every quarter.
  - 1. The Services Division Commander will generate a random number once per quarter that corresponds to the random selection system used to monitor compliance with policy. The Services Commander will be responsible to generate an electronic computer history associated with every departmental employee assigned to the chosen group.
  - 2. The computer history provides a detailed account of all computer activity that occurred on the department employee's profile during the selected time frame. This includes a list and categorization of all sites on the World Wide Web which were visited during the time frame. The report will also provide a detailed history depicting the type and amount of data downloaded from each site.
  - 3. The Services Commander or his designee will be responsible to research each report and determine appropriate compliance with policy. All misconduct with respect to the use of the MDT or other computerized equipment will be managed in accordance with the Department's disciplinary policy: [1104.03---Disciplinary Process](#).
  - 4. Supervisory personnel within the agency may request a computer history report associated with an employee falling within their span-of-control at any time without advanced notice. Consistent with Section G Paragraph 3 above, the Services Commander or his designee will remain responsible to generate all computer history reports requested by supervisory personnel.
- H. **The safe operation of the police vehicle takes priority over the operation of the MDC.** Operation of the MDC will not be considered a mitigating justification in the event of a traffic accident. While undertaking MDC operations, personnel will maintain a conscious awareness of their surroundings, remain alert to potential hazards and employ safe tactics. Officers will stop at a secure parking location when extended MDC usage is anticipated.
- I. In order to protect the computer unit, the MDC must be turned off (signed off and powered down) if the police vehicle must be "jump started".
- J. All MDC's have been configured to accept a standard user name and password. When officers in the field access the Texarkana Police Department's network server, the officer must access the server utilizing their individual username and respective password. Officers shall log onto their MDC at the beginning of their shift.

Page 2 of 3    Number: 1109.02	Effective Date: March 18, 2011
Subject: Mobile Data Computers	<b>Revision Date: March 12, 2015</b>

- K. Officers in the field wishing to connect to the ACIC inquiry function must utilize the username (CSN number) and applicable password issued through ACIC to access the system. All such users must first receive Level 1 certification through the Arkansas Crime Information Center (ACIC) before such information is issued to the officer.
- L. Security of the MDC is of extreme importance to the Texarkana Police Department. Any actions which may compromise the security of the system will not be tolerated. Security of the MDC is the responsibility of the officer who is logged on. Although not inclusive, examples of security breaches are identified below:
  - 1. Sharing or disclosing network usernames and/or passwords to unauthorized individuals. For additional information regarding network usernames and passwords, please refer to [General Order 1109.01---Use of Computer Equipment, Email and Internet Access](#) .
  - 2. Sharing or disclosing CSN numbers and/or passwords associated with ACIC connectivity with unauthorized individuals.
  - 3. Utilizing another user's account, username, password or CSN number.
  - 4. Leaving the MDC unattended and unsecured while operational.
- M. The MDC shall remain operational during the officer's tour of duty. Officers shall maintain contact with the Central Communications Section and remain ready to accept all assigned calls for service.
- N. The MDC shall be properly shut-down, and the officer shall log out of the system at the conclusion of his/her tour of duty.
- O. Instructions regarding procedural operations of MDCs such as how to log on, how to run inquiries, or commands for operating the MDC must not be broadcast by voice radio transmissions in an effort to prevent unauthorized persons who may be monitoring Texarkana Police Department's radio frequencies from gaining a working knowledge of the MDC system.
- P. No food or drink will be placed on or near an MDC. Officers are responsible for all damage that occurs to the MDC assigned within their respective unit. Should officers encounter a damaged or non-functioning MDC, the officer shall notify his/her immediate supervisor of the circumstances.
  - 1. The supervisor will remain responsible to ensure the officer is placed within another police unit with a functioning MDC, and in those instances that involve damage to the MDC, the supervisor shall ensure appropriate information is sent to the Services Division Commander through the established chain-of-command.

**V. Routine Calls for Service**

- A. On routine calls for service, personnel in the Central Communications Section will use voice transmission to relay the call to the unit or units to be assigned. CAD information will be sent via the MDC system. The assigned units will acknowledge the assignment by voice transmission and by pressing the appropriate MDC function key that signals their acknowledgement.
- B. Upon arrival at the scene, officers will verbally notify the dispatcher and press the appropriate MDC function key that signals the officer's arrival at the scene of a call for service.
- C. Upon completion of the call, the primary officer is responsible for entering the appropriate disposition code into the MDC.
- D. For additional guidance and information relating to answering calls for police service, refer to [General Order 1105.03--- Routine Calls for Service](#).

Page 3 of 3    Number: 1109.02	Effective Date: March 18, 2011
Subject: Mobile Data Computers	<b>Revision Date: March 12, 2015</b>