CHAPTER 19

MOBILE DIGITAL COMPUTER OVERSIGHT AND USE

REVISED JULY 2020

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 19

MOBILE DIGITAL COMPUTER OVERSIGHT AND USE

1. PURPOSE. The purpose of this chapter is to provide policy regarding the oversight and mandatory use of departmental mobile digital computers (MDC).

2. DEFINITION.

a. An MDC is defined as a semi-rugged computing device (i.e., laptop, tablet, Windows control module in a patrol vehicle) that can endure more rigorous operations. Its use is exclusively for uniformed personnel (specifically officers and sergeants) for the purpose of communications with the Department's Computer Aided Dispatch (CAD) application and the generation of field reports. An MDC differs from standard or administrative computing devices as it is configured to operate on the CAD network and the Department's local area network.

b. Advanced authentication, also known as two-factor authentication, provides additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, smart ID cards, and software tokens. Advanced authentication employs the use of two of the following three factors of authentication: something you know (e.g., password), something you have (e.g., hard token), something you are (e.g., biometric). The two authentication factors shall be unique, such as password/token or password/biometric.

c. A user is defined as an officer or sergeant.

3. BACKGROUND.

a. Mobile Digital Computer. The MDC is a valuable tool for communication which enables full functionality of several built-in officer safety components, especially in a patrol vehicle. For the equipment and application to work as designed, the Consolidated Patrol Vehicle Environment (CPVE)/MDC shall be on and connected to the network with the global positioning system (GPS) enabled, and the user properly logged into the CAD application with their six-digit ID number and call-sign.

(1) Computer Aided Dispatch Application. In the event the "9-1-1" button in the CAD application is pressed:

(a) Patrol Vehicle. The CPVE/MDC equipment and CAD application in the patrol vehicle will automatically provide dispatch with an "SOS" alert, including the patrol vehicle's license plate number and geographical location, and the user's call-sign, six-digit ID number, and name.

(b) Tablet and Laptop. The device will automatically provide dispatch with an "SOS" alert; its geographical location; and the user's call-sign, six-digit ID number, and name.

NOTE: If a user is not logged into the CAD application, the "9-1-1" button is not enabled and, therefore, dispatch will not be alerted.

(2) Portable Radio. In the event the "11-99" button is pressed on the portable radio, the CPVE/MDC equipment and CAD application will provide dispatch with an "11-99" alert and the patrol vehicle's GPS location.

b. Advanced Authentication. Criminal Justice Information System (CJIS) mandates advanced authentication requirements under certain circumstances. The CJIS requirements allow for a username and password when used in a secure location, such as a building with controlled access or a computer in a patrol vehicle when physically secured to the vehicle. All marked departmental patrol vehicles with trunk-mounted computer systems meet the CJIS minimum requirements. Patrol vehicles equipped with tablets or mounted MDC laptops do not meet the requirements set forth by the CJIS mandate; therefore, advanced authentication has been implemented for these devices.

4. OVERSIGHT OF MOBILE DIGITAL COMPUTER RESOURCES. The Information Management Division (IMD) is responsible for the oversight of the MDC hardware. To fulfill this responsibility, IMD has established policy to ensure the proper application of software licenses, overall accountability of MDCs, and tracking and monitoring of all associated hardware. The IMD is responsible for support and administration of all MDCs, including configuration, setup, and asset management. Additionally, IMD shall ensure all MDCs not permanently mounted within the patrol vehicle utilize advanced authentication (i.e., fingerprint reader) as an additional security measure.

5. MOBILE DIGITAL COMPUTER USE POLICY. This policy applies to MDC use for all headquarters, Division, and Area commands. Commands shall comply with all of the following:

a. The MDCs (i.e., tablet and laptop) designed to be utilized in multiple environments, thus allowing officers to operate the MDC in and away from the patrol vehicle, shall be:

(1) Stored in a secure location.

(2) Equipped with advanced authentication.

b. All uniformed employees (i.e., sergeants and officers) on-duty, including overtime details, in a marked patrol vehicle, shall:

(1) Login to the patrol vehicle's MDC and CAD application using their assigned unit ID at the start of the shift or overtime detail to enable the GPS.

(2) Remain logged in until the end of the shift or overtime detail.

c. Ensure the full quantity of MDCs provided to each command are available to every officer and sergeant on-duty and working in an enforcement capacity.

d. Ensure MDCs provided are exclusively for use by officers and sergeants assigned to enforcement duties in the field. Employees, of any rank or classification, shall not deprive field uniformed personnel of an MDC (i.e., tablet or laptop) by allocating this resource for administrative purposes. If administrative laptops are required, commands should request laptops following current procurement procedures (refer to Highway Patrol Manual 11.2, Materials Management Manual, Chapter 17, Information Technology Goods and Services Acquisition).

e. In the event a patrol vehicle is not equipped with a functioning MDC, or the user is unable to login, the user shall notify their supervisor or manager immediately and utilize another patrol vehicle with a functioning MDC. If there is no patrol vehicle available with a functioning MDC, the user shall advise the appropriate communications center of the following:

(1) The unit ID of the patrol vehicle with the inoperable MDC.

(2) The name of supervisor or manager notified.

THIS PAGE INTENTIONALLY LEFT BLANK