GENERAL ORDER

Loudoun County Sheriff's Office

Chapter: Operations		**Section:** 401.16
Subject: Operational Functions		**Topic:** MDCs and Other Electronic Equipment
Accreditation: OPR. 01.06		**Revised:** **Reaffirmed:**
Enacted: 07/30/2015	**Last Review:** 07/24/2015	**Review:** 07/30/2016

I. PURPOSE

The purpose of this General Order is to establish guidelines for the use of mobile computers, cellular telephones, and other mobile communications.

II. POLICY

It is the policy of this agency to develop and provide effective and reliable technology to all members of the department and to provide increased efficiency in communications, report writing, and other automated tasks through the use of mobile computers and cellular telephones.

III. DEFINITIONS

A. Mobile Data Computer (MDC): The hardware device, usually a laptop computer, which is used by officers in the field to write offense reports, request inquiries through VCIN/NCIC, and operate other approved software applications. (Mobile Data Computer (MDC) and Mobile Data Terminal (MDT) are interchangeable terms.

B. Vehicle Mounts: A system of hardware and brackets used to hold the computer system in the vehicle.

C. Mobile Communication: Cellular telephones, pagers, etc.

D. NCIC: National Criminal Information Center

E. VCIN: Virginia Criminal Information Network

F. TSPD: Technology Section P.D./Administrative and Technical Services Division

G. DIT: Department of Information Technology

H. GEAC: Software used for report writing, accident reports, and VCIC/VCIN.

I. VRM: A mobile data modem used to transmit information over the radio frequency.

J. VIBR: Virginia Incident Based Reporting.

K. Flash drive: A removable storage device that plugs into a USB port on the MDC.

L. Shared workstation: Any computer in the deputy work rooms or sergeant's offices that are not assigned to a specific user or function.

M. PME: Encryption software installed on MDC's and shared work stations. PME will encrypt any disc or flash drive used on a computer when the software has been installed on that computer.

N. Emergency Incidents: Priority one (1) or two (2) incidents requiring an immediate, "Code Three" response as defined in General Order 405.2.

O. Medium Risk Incidents: Incidents having the potential of turning into an emergency incident or requiring a two-unit response.

P. Low Risk Incidents: Incidents where officer/public safety is at a low risk of being threatened.

IV. TRAINING AND SECURITY

A. Only individuals who have been trained on the software application for the mobile data computers are authorized operators.

1. The TSPD will ensure that selected officers are trained in all aspects of the mobile software, to include report writing and accident forms.

2. Passwords will be issued by the Department of Information Technology and will be used only by the assigned deputy. No other passwords will be used unless approved by a DIT representative or a TSPD Administrator.

B. VCIN/NCIC Operations Procedures

1. Information obtained through VCIN/ NCIC is for criminal justice purposes only and may not be disseminated or provided to non-criminal justice personnel, unless otherwise prescribed by law.

2. Each agency that transmits requests through the mobile digital terminal shall use their agency's own specific ORI (identification) number.

3. The MDC may have access to the VCIN system only when installed in a Sheriff's vehicle or when operated in a law enforcement facility. If the MDC is removed from the vehicle or not operated in a law enforcement facility, the VCIN connection shall not be used except for emergency law enforcement purposes.

4. Data received through the VCIN system shall not be stored within the computer system for later retrieval except for that information required to be maintained regarding mobile terminals. Data needed for future use shall be re-retrieved from the VCIN system.

5. MDC's may be used to communicate from car-to-car, car-to-base and, except for criminal histories, inquire into the databases of the VCIN/NCIC and NLETS (National Law Enforcement Telecommunications System).

6. Deputies using MDC's will ensure that no unauthorized person can view information on the mobile computer screen.

7. Deputies will ensure that MDC's are only used in a secure area, such as in a Sheriff's vehicle or under the deputy's immediate control if used outside of the Sheriff's vehicle, so as to prevent unauthorized persons from accessing the NCIC/VCIN systems. If left unattended, the mobile computer must be locked in a secure setting, such as a locked Sheriff's vehicle or within the docking station in the locked position. If the MDC is lost or stolen, the agency shall disable the MDC's access to the VCIN system and notify the appropriate division commander immediately in writing.

8. Criminal history reports shall not be transmitted to a mobile terminal.

9. Individuals using MDC's must achieve a minimum of a Level C VCIN certification prior to accessing the VCIN queries.

C. Deputies are reminded that all information sent over the MDC is recorded and can be retrieved for review.

D. If a MDC is in need of repair, the deputy shall leave it in an area designated by a TSPD Administrator along with a brief description of the problem.

1. If a MDC becomes lost or stolen, an IBR report must be completed with a copy forwarded to the TSPD Administrator. If a MDC becomes damaged, a memorandum must be written and submitted to the appropriate supervisor, with a copy forwarded to the TSPD Administrator.

2. When leaving a Sheriff's vehicle at the county garage or other location, the MDC shall be removed by the deputy prior to relinquishing control of the vehicle, and thereafter kept in a secure location.

V. COMPUTER GUIDELINES

A. Only the Department of Information Technology or TSPD Administrator has authority to load any software on the MDC.

1. Only the Department of Information Technology or TSPD Administrator has the authority to add, delete, or modify any software loaded into the MDC. The operation and/or loading of personal software is prohibited.

2. The hard drive may be used to save or store documents or information but the use of a flash is recommended.

B. Deputies will not place any food, drink, or other item directly on the computer or in a location that may cause liquid or food to be spilled onto/into the computer.

C. While operating a Sheriff's Office vehicle, laptop computers and other data technology devices, to include programming GPS devices, shall not be used by the driver while the vehicle is in motion.

VI. DATA STORAGE PROCEDURES

A. The hard drive of a MDC or shared workstation may be used to save or store any files needed by a user to do his/her job with the exception of report files. All report files must be saved to a flash drive.

B. PME software is installed on the MDCs and shared work stations. When a disc or flash drive is used in an MDC or shared work station, the data is decrypted and no password is needed. When a floppy disk or flash drive is used on a work station that does not have PME installed, the user will have to provide a password before the data can be accessed.

1. Users who have been issued a CF-30 must use agency-issued flash drives.

2. Once the flash drive has been set up with a password, the password is not to be changed by the user at any time. If, for some reason, the password has been compromised, the user must bring the flash drive to TSPD and have the password updated.

3. Contact TSPD if a password is forgotten.

4. Users who have been issued CD/DVD drives may not use these drives to save reports.

VII. DATA COMMUNICATIONS PROCEDURES

A. The mobile computer will be used for the routine communications of the following:

1. Instant messages

2. Status changes

3. Marking en route and on scene of complaints

4. Changing locations

5. Marking available

a. Prior to marking available, deputies will type in the appropriate disposition in the notes section and deputies will use the "Notes" area whenever possible to document information about the disposition or any actions taken during the complaint;

6. Other information between dispatchers and deputies

7. Marking on and off duty

B. Deputies will not dispatch themselves to waiting calls or respond to calls not dispatched. Deputies will take all call assignments from the dispatcher.

C. Under no circumstances shall an MDC be used to mark out on incidents involving the following:

1. A "Code Three" response as defined in General Order 405.2

2. Pursuits

3. Traffic stops

4. An immediate response for additional units

D. After the initial traffic stop, all non-emergency follow-up communication may be made using the MDC. All other calls may be cleared using the MDC.

E. Deputies may utilize the MDC for marking out on low risk incidents that include, but are not limited to, the following:

1. Low risk follow up on incidents/cases not involving suspects

2. Parking violations

3. Vehicle maintenance

4. Selective enforcement

5. Public service transports

6. Breaks

7. Administrative assignments

8. Disabled vehicles

F. Deputies may utilize the MDC for marking out on medium risk incidents that include, but are not limited to, the following:

1. Building checks/foot patrols

2. Meal breaks

3. Crashes/Hit and run's

4. Warrant services/Petition services

G. Deputies are reminded that the utilization of the MDC for marking out on incidents is at the deputy's discretion and, if doubt exists as to the nature and risk, the radio shall be used.

H. Information that is sent using the instant messenger feature should be limited to short messages that are appropriate in nature. Messages shall be kept to a minimum and pertain to work-related issues only. Generally, if the message would be inappropriate for the radio, it would be inappropriate for the computer. The instant messenger feature will not be utilized to obtain VCIN/NCIC queries from either another vehicle or ECC personnel.

VIII. EMERGENCY COMMUNICATIONS CENTER PROCEDURES

A. Dispatchers

1. Dispatching Calls for Service

a. Emergency incidents include incidents in progress such as murder, rape, robbery, burglary, felonious assault, shots fired, Signal 1, aggravated domestic disputes, etc. This response shall always be radio dispatched to

the assigned units with two alert tones. The assigned units shall acknowledge their response on the radio. Dispatchers will include the following information in their broadcast:

1. Nature, location, and details of incident

2. Units dispatched

3. Notification to patrol duty supervisor

b. Medium risk incidents include incidents such as alarms, non-aggravated domestic disputes, warrant service, suspicious vehicles/persons/events, loud music/noise, disorderly subjects, etc. These incidents may pose a threat to an officer or public safety risk. This response shall be assigned and acknowledged by MDC and voiced over the radio. Dispatchers shall:

1. Assign the call to the designated unit(s)

2. Voice over radio the unit, nature, sector area, location, brief notes, and current time. Units are not required to acknowledge the assignment on the radio

3. Allow 30 seconds for the unit to acknowledge by MDC

c. Low risk incidents include incidents such as disabled vehicles, parking complaints, crimes that occurred in the past (larceny, destruction of property, etc.), runaways, etc. These incidents shall be assigned and acknowledged by MDC and voiced-over the radio at the discretion. Units are not required to acknowledge the assignment on the radio.

2. Emergency Communications Center personnel should be aware that units responding to a call for service may use the radio or MDC to acknowledge calls for service. Any additional supplemental information or pertinent information received that could affect officer safety (such as caution notes, etc.) shall be voice dispatched.

B. Deputies

1. Dispatching

a. Computer Dispatch

The Emergency Communications Center will assign a call for service first, allow sufficient time for the unit to acknowledge the call by activating the "en route" button, and then voice the call on the radio (i.e., "Unit 220A en route for an alarm at 123 Main Street"). This procedure will be used when the unit is equipped with an MDC.

b. Radio Dispatch

The Emergency Communications Center will contact a unit by its designated number, assign the call, and the unit will then acknowledge on the radio (i.e., "Unit 220A, copy an alarm"). The unit will then verbally acknowledge the call on the radio. This procedure will be used for non-MDC units and, in the event the system is out of service.

2. Arriving

a. Units will use the "on scene" button on the MDC to mark on scene.

3. Clearing

a. The primary unit will enter the clearance codes and applicable incident notes using the "Notes" feature and clear the call for service via MDC.

b. The backup unit will utilize the "available" button and return to service.

4. Changing Unit Location

b. When changing unit location (i.e., taking a prisoner to the jail, etc.) the unit may use the "UL" feature. In the "Home" line, the deputy will type, "UL.ENRT ADC" (or other location). The deputy may not use the "en route" button.

b. When arriving at the new location, the unit may use the "UL" feature. In the home line, the deputy will type, "UL.ADC" (or other location). The deputy may not use the status button "onscene".

5. Marking On and Off Duty

a. Any deputy who utilizes a MDC during his/her tour of duty and are assigned a unit designator (i.e., Sergeant, Lieutenant, Crash Reconstruction Unit, Truck Safety Unit, K-9 Unit, etc.) shall use the MDC for marking on duty.

1. To mark on duty, deputies shall log onto EnRoute Mobile and then press the "available" button. This will bring the deputy on duty with dispatch and may be verified by viewing the status indicator at the bottom of the screen.

b. Any deputy who uses a Mobile Data Computer during his/her tour of duty shall use the MDC for marking off duty.

1. To mark off duty, deputies should press the "Off Duty" button. This should show that the unit is "OUT SERV". The unit may then log off EnRoute Mobile.

6. Back-Up Feature

a. Deputies may utilize the "BU" command or "Backup" button to mark out as a backup unit on another unit's call without voicing the information over the radio.

1. Where the "unit number" is listed, the deputy will type in the primary deputy's unit number under "BU.unit number." This will place the deputy in the dispatched status.

2. If en route to another deputy's call, press the "en route" status button.

3. If on scene of another deputy's call, press the "on scene" status button.

b. Patrol supervisors are responsible for monitoring the usage of this feature and enforcing any abuse or unnecessary usage of the feature.

IX. REPORT WRITING

A. Deputies

1. Unless otherwise directed by a supervisor, all deputies who have been trained in the application of the reporting software for both the accident (FR300) and incident-based reporting (IBR) will use the mobile computer for the generation of these reports.

2. After completing a report, the deputy will electronically sign the report in the reporting officer's section only. Deputies are specifically prohibited from

signing or approving the report in the supervisor's section unless they have approving authority.

3. Once the report has been signed, the deputy will electronically transmit the report to his/her supervisor or approving authority for review and endorsement. Deputies will ensure that completed reports are sent to an on-duty supervisor for review.

B. Supervisors

1. Supervisors will electronically retrieve reports awaiting approval. They shall review and approve the reports using the report software.

2. After the review, the supervisor will electronically sign the approved report and transmit it to the Records Section.

3. If a supervisor finds a mistake in a report, the note section of the reporting software will be used to describe the mistake(s). The report will be electronically returned to the reporting deputy for corrections. It will be the responsibility of the reporting deputy to correct the mistakes and re-send the report to the supervisor for final approval.

4. Once a report has been transmitted to the Records Section, the report will not be retrieved for any changes. Any further corrections will have to be made through the Records Section supervisor or by completing a supplemental report.

X. MOBILE COMMUNICATIONS/ELECTRONIC DEVICES

A. Unauthorized Technology in County-Owned Vehicles

1. No non-Loudoun County Sheriff's Office issued communication or electronic device shall be hard-wired in any county-owned vehicle.

2. No personal video entertainment device shall be used or operated by agency personnel while on duty or while occupying/operating a county-owned vehicle. A personal video entertainment device may include, but is not limited to, DVD players, portable televisions, laptop computers, hand-held electronic games, etc.

B. While operating a Sheriff's Office vehicle, personal or issued cell phones shall not distract a sworn or civilian employee from the safe operation of the vehicle.

C. Sheriff's Office issued cell phones shall be kept charged and in working order.

D. Personal calls on Sheriff's Office issued cell phones should be kept to a minimum.