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 using 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. TSS: Technology Services Section

G. DIT: Department of Information Technology

H. VIBR: Virginia Incident Based Reporting.

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

J. Shared workstation: Any computer that are not assigned to a specific user or function.

K. Emergency Incidents: Priority one (1) or two (2) incidents requiring an immediate, “Code Three” response as defined in General Order 405.2.
L. 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 TSS will ensure that deputies are trained in all aspects of the mobile software, to include report writing and accident forms.

2. Passwords will adhere to the Department of Information Technology standards and shall not be shared.

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 VCIN shall not be stored or saved on a computer system or server 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. DMV/VCIN/NCIC data shall not be copied and pasted into any computer program. This includes copying DMV/VCIN/NCIC data into the comments of CAD incidents.

6. MDCs may be used to communicate from car-to-car, car-to-dispatch and, except for criminal histories, inquire into the databases of the VCIN/NCIC and NLETS (National Law Enforcement Telecommunications System).
7. Deputies using MDCs will ensure that no unauthorized person can view information on the mobile computer screen.

8. Deputies will ensure that MDCs 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, 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 deputy shall immediately notify their supervisor and TSS. The TSS supervisor shall disable the MDCs access to county network systems, VCIN system, and notify the appropriate division commander immediately in writing.

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

10. Individuals using MDCs 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 an MDC needs repair, the deputy shall leave it in an area designated by a TSS Administrator along with a brief description of the problem.

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

2. When relinquishing control of a Sheriff’s vehicle to a non-sworn individual (such as maintenance), 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 DIT or the TSS Administrator have the authority to install software on the MDC.

1. Only DIT or the TSS Administrator has the authority to add, delete, or modify software on 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 Microsoft Office365 OneDrive or SharePoint is recommended.
3. Use of external drives (flash/thumb drives) is not recommended as they are not encrypted and data on external media can easily be lost or stolen.

4. Only flash drives purchased by the TSS may be used in agency computers. To prevent virus infections, flash drives obtained from the public may not be used.

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

1. While operating a Sheriff’s Office vehicle, laptop computers, wireless communication devices, GPS devices, and any other device that could create a distraction shall not be used by the driver while the vehicle is in motion.

VI. DATA COMMUNICATIONS PROCEDURES

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

1. Instant messages

2. Status changes
   a. En-route
   b. On Scene
   c. Available
   d. Secondary location

3. Other information between dispatchers and deputies

4. Marking on and off duty

5. Self-dispatch to pending incidents

B. 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. An immediate response for additional units
C. All non-emergency communications and requests may be made using the MDC.

D. Deputies may utilize the MDC for initiating incidents that do not involve an emergency response.

E. Information that is sent using the instant messenger or chat 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.

VII. 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. Dispatchers shall 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 by the dispatcher over the radio. Dispatchers shall:

      1. Assign the call to the designated unit(s)
      2. Voice over radio the unit, nature, beat, location, brief notes, and current time. Units are required to acknowledge the assignment on the MDC.
3. Allow 30 seconds for the unit to acknowledge by MDC. If a response is not received by MDC, the dispatcher shall ask for confirmation on the radio.

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 of the dispatcher. Units are required to acknowledge the assignment on the MDC.

2. Emergency Communications Center personnel should be aware that units responding to a call for service may not see comments added after the initial dispatch. 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 pressing 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”).

   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 units that are not equipped with an MDC and in the event the system is out of service.

2. Arriving

   i. Units will use the “on scene” button on the MDC to indicate they are on scene.

3. Clearing
a. The primary unit will enter the appropriate disposition code(s) and applicable incident comments on the MDC.

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

4. Changing Unit Location

ii. When changing unit location (i.e., taking a prisoner to the jail, etc.) the unit shall change their status using the status change feature on the MDC to include destination location.

b. When arriving at the new location, the unit shall update their status and location using the status change feature on the MDC.

5. Marking On and Off Duty

a. Any deputy who utilizes a MDC during his/her tour of duty shall use the MDC for marking on duty.

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

6. Back-Up Feature

a. Deputies may utilize the “Backup” button to mark out as a backup unit on another unit’s call without voicing the information over the radio.

VIII. REPORT WRITING

A. Deputies

1. Deputies shall utilize agency software to complete all required reports.

2. Once the report has been completed, the deputy shall electronically transmit the report to his/her supervisor or approving authority for review and endorsement.

B. Supervisors

1. Supervisors shall review and approve the reports using the report software.

2. After the review, the supervisor will electronically approve the report and transmit it to the Records Section.
3. If a supervisor finds a mistake in a report, they shall provide guidance and electronically return the report to the reporting deputy for corrections. It will be the responsibility of the reporting deputy to correct the mistakes and re-submit the report to the supervisor for final approval.

4. Once a report has been transmitted to the Records Section, the report cannot be retrieved for any changes. Any further corrections require a supplemental report.

IX. 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 agency issued wireless communication devices 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.