Mobile Data Browser Use

424.1 PURPOSE AND SCOPE

The purpose of this policy is to establish guidelines for the proper access, use and application of the Mobile Data Browser (MDB) system in order to ensure proper access to confidential records from local, state and national law enforcement databases, and to ensure effective electronic communications between office members and Emergency Communications Center.

424.2 POLICY

St. Mary's County Sheriff's Office members using the MDB shall comply with all appropriate federal and state rules and regulations and shall use the MDB in a professional manner, in accordance with this policy.

424.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy regarding messages accessed, transmitted, received or reviewed on any office technology system (see the SMCG Information Technology Use and Security Policy via the Intranet for additional guidance).

424.4 RESTRICTED ACCESS AND USE

MDB use is subject to the Information Technology Use Policy.

Members shall not access the MDB system if they have not received prior authorization and the required training. Members shall immediately report unauthorized access or use of the MDB by another member to their supervisors or Shift Supervisors.

Use of the MDB system to access law enforcement databases or transmit messages is restricted to official activities, business-related tasks or for communications that are directly related to the business, administration or practices of the Office. If a member has questions about sending a particular message or accessing a particular database, the member should seek prior approval from his/her supervisor.

Sending offensive, demeaning, derogatory, defamatory, obscene, disrespectful, sexually suggestive, harassing or any other inappropriate messages on the MDB system is prohibited. Any message containing slang or language which could be construed as a slur or sexual harassment against any person or group will not be tolerated. All transmissions are recordable, retrievable and are public record. Any of the above is likely to result in discipline.

It is a violation of this policy to transmit a message or access a law enforcement database under another member's name or to use the password of another member to log in to the MDB system unless directed to do so by a supervisor. Members are required to log off the MDB or secure the MDB when it is unattended. This added security measure will minimize the potential for unauthorized access or misuse.

All user operations will comply with the St. Mary's County Government IT Policy and Procedure, Chapter 5 "Use and Security" policy. The policy is located at http://intranet/.

All MDB operations shall be in accordance with the SMCSO Mobile Data Browser Standard Operating Procedures.

For procedures related to Restricted Access and Use, see the St. Mary's County Sheriff's Office LE Procedures Manual: System Security and Mobile Data Browser General Procedures

424.4.1 USE WHILE DRIVING

Use of the MDB by the vehicle operator should be limited to the times when the vehicle is stopped. Information that is required for immediate enforcement, investigative, tactical or safety needs should be transmitted over the radio.

Safe operation of the patrol vehicle is paramount. It is stressed that common sense and safe driving practices dictate the Deputy Sheriff shall focus his/her attention on safe operation of the vehicle and view the MDB only when the vehicle is not in motion and is safe to do so.

424.5 RESPONSIBILITIES

424.5.1 COMMANDER RESPONSIBILITIES

The Sheriff or Assistant Sheriff shall designate a Division Commander for the agency's management and operations of the MDB Program to include training, maintenance, and repair of all equipment as well as communication and interaction between Federal, State, and local agencies that support the MDB Program.

424.5.2 IT RESPONSIBILITIES

The St. Mary's County Government Information Technology Department (IT) will be responsible for the daily administration of the MDB Program. Additionally, IT will conduct random administrative security checks of the MDB system to ensure that all necessary security procedures are being followed.

424.6 DOCUMENTATION OF ACTIVITY

Except as otherwise directed by the Shift Supervisor, all calls for service assigned by a dispatcher should be communicated by voice over the sheriff's radio and/or electronically via the MDB unless security or confidentiality prevents such broadcasting.

MDB and voice transmissions are used to document the member's daily activity. To ensure accuracy:

(a) All contacts or activity shall be documented at the time of the contact.

(b) Whenever the activity or contact is initiated by voice, it shall be documented by a dispatcher.

(c) Whenever the activity or contact is not initiated by voice, the member shall document it via the MDB.

424.6.1 STATUS CHANGES

All changes in status (e.g., arrival at scene, meal periods, in service) will be transmitted over the sheriff's radio or through the MDB system.

Members responding to in-progress calls shall advise changes in status over the radio to assist other members responding to the same incident. Other changes in status can be made on the MDB when the vehicle is not in motion.

424.7 EQUIPMENT CONSIDERATIONS

(a) Wireless mobile computing devices may interfere with the function of inadequately protected medical devices, including pacemakers.

(b) Wireless mobile computing device users will be mindful of regulations governing the use of the device. The user will deactivate the device in areas where radio devices are forbidden, or when it may cause interference or danger. Any restrictions on use pertaining to cell phones and two-way radios will apply to the MDB. Similar to radio transmission, special attention should be used in the following areas: fuel depots, chemical plants, blasting operations, and other areas where radio transmissions are restricted.

For procedures related to Equipment Considerations, see the St. Mary's County Sheriff's Office LE Procedures Manual: Care of Equipment

424.7.1 MALFUNCTIONING MDB

Whenever possible, members will not use vehicles with malfunctioning MDBs. Whenever members must drive a vehicle in which the MDB is not working, they shall notify the Emergency Communications Center. It shall be the responsibility of the dispatcher to document all information that will then be transmitted verbally over the sheriff's radio.

424.7.2 BOMB CALLS

When investigating reports of possible bombs, members should turn off their MDBs when in close proximity of a suspected explosive device. Radio frequency emitted by the MDB could cause some devices to detonate.

424.8 PROHIBITED USES

(a) MDBs contain sensitive law enforcement information. Use of or access to the MDB's by unauthorized persons is prohibited.

(b) The unauthorized introduction of software programs or other files or, the manipulation or alteration of current software running on agency-owned mobile, desktop or hand-held computers is strictly prohibited.

(c) All MDB data and software maintained or used by the St. Mary's County Sheriff's Office are for official use only. Deputy Sheriffs shall not use or cause to be used any MDB for personal gain or benefit of any kind.

(d) Deputy Sheriffs shall not attempt to install, delete or modify any software or hardware associated with the MDB at any time.

(e) Deputy Sheriffs may not access information concerning individuals who are not the subject of legitimate police inquiries.

(f) Violations of prohibitions may result in disciplinary action and/or criminal prosecution.

424.9 SOFTWARE/HARDWARE

(a) Only software purchased or acquired by the county will be installed on MDBs. IT personnel or an IT approved contractor will handle all software installation or MDB repairs. The introduction, download or installation of any software (i.e., games, music, screen savers, wallpaper, etc.) without prior approval is strictly prohibited.

(b) IT shall install and/or ensure antivirus updates are current.

(c) All electronic messaging/correspondence is the property of St. Mary's County Government. Any electronic message which is sent through the MDB system may be retrieved by authorized personnel later, even though it may have been deleted from the assigned employee's MDB. Electronic messages are not a protected form of communication and could be subject to a discovery motion in a criminal/civil case or an internal administrative investigation.

424.10 WARRANT VERIFICATION

(a) Special care must be taken in using the MDB to check warrants. Not all local warrants have been entered into the HTE database. The absence of a warrant in the system does not necessarily mean there are no local warrants. The Deputy Sheriff must still have the Station Clerk confirm an active warrant.

(b) Warrant information received from the MDB will not be considered probable cause for arrest. Warrant HIT confirmation steps include:

1. Deputy Sheriffs receiving a HIT on his/her MDB shall verify the HIT by viewing the NCIC summary screen to ensure the HIT is for the person or type of property and identical information they requested, prior to initiating a stop, contact or other law enforcement activity, unless other probable cause exists for the stop.

2. Deputy Sheriffs shall confirm a warrant HIT through ECC or the Station Clerk prior to making an arrest or recovery. Waiting for the HIT confirmation does not prohibit the Deputy Sheriff from taking necessary precautions to secure the suspect individual for officer safety.

424.11 CJIS/NCIC/METERS INFORMATION SYSTEMS

(a) CJIS/NCIC/METERS can be accessed via LAN-connected computers. These systems offer detailed information concerning the personal and physical identity of individuals which may be of concern to law enforcement.

(b) Maryland law prohibits secondary dissemination of CJIS information for any reason other than official purposes. This information applies to motor vehicle and licensing information obtained through CJIS. Any person disseminating criminal history record information to unauthorized recipients is subject to Federal and State imposed sanctions.

(c) Only Deputy Sheriffs who have been trained and have authorized access to METERS (Maryland Electronic Telecommunications Enforcement Resource Systems), NCIC (National Crime Information Center) and CJIS (Criminal Justice Information System) may use those criminal history and motor vehicle information files.

(d) Deputy Sheriffs are required to utilize the MDB to make all CJIS/NCIC/METERS inquiries unless circumstances exist which make utilizing the MDB impractical or endanger officer safety.

(e) Responses from inquiries to CJIS/NCIC/METERS are protected information. Deputy Sheriffs are not permitted to utilize these systems for their own personal use. Information received through these computer systems shall only be utilized for official criminal justice purposes necessary to complete a law enforcement or agency objective.

(f) Deputy Sheriffs shall ensure unauthorized persons, including passengers or offenders located within their patrol vehicle, do not view responses from these systems. When the MDB is not in use, the laptop cover shall be closed or covered.

(g) Deputy Sheriffs are responsible for maintaining all certifications, which allow access to CJIS/NCIC/METERS and other databases retrievable by an MDB.