

Protected Information

805.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the access, transmission, release and security of protected information by members of the St. Mary's County Sheriff's Office. This policy addresses the protected information that is used in the day-to-day operation of the Office and not the public records information covered in the Records Maintenance and Release Policy.

805.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of the St. Mary's County Sheriff's Office and is subject to any access or release restrictions imposed by law, regulation, order or use agreement. This includes all information contained in federal, state or local law enforcement databases that is not accessible to the public.

805.2 POLICY

Members of the St. Mary's County Sheriff's Office will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

805.3 RESPONSIBILITIES

The Sheriff shall select a member of the Office to coordinate the use of protected information.

The responsibilities of this position include, but are not limited to:

- (a) Ensuring member compliance with this policy and with requirements applicable to protected information, including requirements for the National Crime Information Center (NCIC) system, National Law Enforcement Telecommunications System (NLETS), Motor Vehicle Administration (MVA) records, Maryland Criminal Justice Information System (CJIS) and Maryland Electronic Telecommunications Enforcement Resource System (METERS).
- (b) Developing, disseminating and maintaining procedures that adopt or comply with the U.S. Department of Justice's current Criminal Justice Information Services (CJIS) Security Policy.
- (c) Developing, disseminating and maintaining procedures necessary to comply with confidentiality and release of information obtained from the Biological Agents Registry Program (BAR) (Md. Code HG § 17-604).
- (d) Developing, disseminating and maintaining any other procedures necessary to comply with any other requirements for the access, use, dissemination, release and security of protected information.
- (e) Developing procedures to ensure training and certification requirements are met.

St. Mary's County Sheriff's Office

LE Policy Manual

Protected Information

- (f) Resolving specific questions that arise regarding authorized recipients of protected information.
- (g) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

805.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, St. Mary's County Sheriff's Office policy or training. Only those members who have completed applicable training and met any applicable requirements, such as a background check, may access protected information, and only when the member has a legitimate work-related reason for such access.

Unauthorized access, including access for other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action pursuant to the Personnel Complaints Policy and/or criminal prosecution.

Deputy Sheriffs are required to use the MDB to make all CJIS/NCIC/METERS inquiries unless circumstances exist that make using the MDB impractical or endanger officer safety.

For procedures related to Access to Protected Information, see the St. Mary's County Sheriff's Office LE Procedures Manual: [Operational Accessibility](#).

805.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may be released only to authorized recipients who have both a right to know and a need to know.

A member who is asked to release protected information that should not be released should refer the requesting person to a supervisor or to the Records Supervisor for information regarding a formal request.

Unless otherwise ordered or when an investigation would be jeopardized, protected information maintained by the Office may generally be shared with authorized persons from other law enforcement agencies who are assisting in the investigation or conducting a related investigation. Any such information should be released through the Records Section to ensure proper documentation of the release (see the Records Maintenance and Release Policy).

Protected information, such as Criminal Justice Information (CJI), which includes Criminal History Record Information (CHRI), should generally not be transmitted by radio, cellular telephone or any other type of wireless transmission to members in the field or in vehicles through any computer or electronic device, except in cases where there is an immediate need for the information to further an investigation or where circumstances reasonably indicate that the immediate safety of deputies, other office members, or the public is at risk.

Nothing in this policy is intended to prohibit broadcasting warrant information.

St. Mary's County Sheriff's Office

LE Policy Manual

Protected Information

For procedures related to Release of Dissemination of Protected Information, see the St. Mary's County Sheriff's Office LE Procedures Manual: [Operational Accessibility](#).

805.6 SECURITY OF PROTECTED INFORMATION

The Sheriff will select a member of the Office to oversee the security of protected information.

The responsibilities of this position include, but are not limited to:

- (a) Developing and maintaining security practices, procedures and training.
- (b) Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.
- (c) Establishing procedures to provide for the preparation, prevention, detection, analysis and containment of security incidents including computer attacks.
- (d) Tracking, documenting and reporting all breach of security incidents to the Sheriff and appropriate authorities.

805.6.1 MEMBER RESPONSIBILITIES

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized to access or receive it. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (e.g., on an unattended table or desk; in or on an unattended vehicle; in an unlocked desk drawer or file cabinet; on an unattended computer terminal).

805.7 TRAINING

All members authorized to access or release protected information shall complete a training program that complies with any protected information system requirements and identifies authorized access and use of protected information, as well as its proper handling and dissemination.