Policy Number: 801 – Protected Information
Effective Date: February 9, 2021
Revision Date: February 9, 2021
Approved By: Brandon Gatlin, Interim Chief of Police

801.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines to members of the Montana State University Billings Police Department (Department) regarding the access, transmission, release and security of protected information. This policy addresses the protected information used in the day-to-day operation of the Department and not the public records information covered in Department Policy 800 - Records Maintenance and Release.

801.1.1 DEFINITIONS

Definitions related to this policy include:

Protected information - Any information or data that is collected, stored or accessed by members of this Department 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.

801.2 POLICY

Members of this Department will adhere to all applicable laws, orders, regulations, use agreements and training related to the access, use, dissemination and release of protected information.

801.3 RESPONSIBILITIES

The Chief of Police, or their designee, shall coordinate the Department's use of protected information.

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

1. 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 Division (MVD) records and Montana Criminal Justice Information Network (CJIN).
2. 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.
3. 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.

4. Developing procedures to ensure training and certification requirements are met and maintained.
5. Resolving specific questions that arise regarding authorized recipients of protected information.
6. Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

801.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Department 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 anything other than a legitimate work-related purpose, is prohibited and may subject a member to administrative action and/or criminal prosecution.

801.5 RELEASE OR DISSEMINATION OF PROTECTED INFORMATION

Protected information may only be released 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.

Unless otherwise ordered, or when an investigation would be jeopardized, protected FERPA information maintained by the Department may generally be shared with authorized persons from other law enforcement agencies. Any such information should be released only after authorization from a supervisor to ensure proper documentation of the release (see Department Policy 800 - Records Maintenance and Release).

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. Caution should also be exercised before transmitting in a vehicle 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 officers, other Department members or the public is at risk.

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

801.6 SECURITY OF PROTECTED INFORMATION

The Chief of Police, or their designee, will oversee the security of protected information. The responsibilities of this position include, but are not limited to:

1. Developing and maintaining security practices, procedures and training.
2. Ensuring federal and state compliance with the CJIS Security Policy and the requirements of any state or local criminal history records systems.
3. Establishing procedures to provide for the preparation, prevention, detection, analysis and containment of security incidents including computer attacks.
4. Tracking, documenting and reporting all breach of security incidents

801.6.1 MEMBER RESPONSIBILITIES

Members accessing or receiving protected information shall ensure the information is not accessed or received by persons who are not authorized. This includes leaving protected information, such as documents or computer databases, accessible to others when it is reasonably foreseeable that unauthorized access may occur (i.e. 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).

801.7 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.