Protected Information

806.1 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 Beltrami 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 government data information covered in the Records Maintenance and Release Policy.

806.1.1 DEFINITIONS

Definitions related to this policy include:

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

806.2 POLICY

Members of the Beltrami 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.

806.3 RESPONSIBILITIES

The Sheriff shall select a member of the Office to coordinate the use of protected information (Minn. Stat. § 13.05, Subd. 13).

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, the National Law Enforcement Telecommunications System (NLETS), Minnesota Division of Driver and Vehicle Services (DVS) records, Minnesota Bureau of Criminal Apprehension (BCA) and the Minnesota Comprehensive Incident-Based Reporting System (CIBRS).

(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 any other procedures necessary to comply with any other requirements for the access, use, dissemination, release and security of protected information.

(d) Developing procedures to ensure training and certification requirements are met.

(e) Resolving specific questions that arise regarding authorized recipients of protected information.

(f) Ensuring security practices and procedures are in place to comply with requirements applicable to protected information.

(g) Ensuring a comprehensive security assessment of any personal information maintained by the Beltrami County Sheriff's Office is conducted at least annually (Minn. Stat. § 13.055, Subd. 6).

(h) Ensuring CIBRS is notified within 10 days that an investigation in CIBRS has become inactive (Minn. Stat. § 299C.40).

806.4 ACCESS TO PROTECTED INFORMATION

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Beltrami County Sheriff's Office policy or training (Minn. Stat. § 13.09). 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 (Minn. Stat. § 13.05; Minn. Stat. § 299C.40).

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.

806.5 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 Center 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.

806.5.1 REVIEW OF CHRI

Members of this office shall refer individuals seeking access to CHRI to the Minnesota BCA (Minn. Stat. § 13.87, Subd. 1(b)).

806.5.2 REVIEW OF CIBRS DATA

An individual who is the subject of private data held by CIBRS may request access to the data by making a request to the Records Supervisor. If the request is to release the data to a third party, the individual who is the subject of private data must appear in person at the Office to give informed consent to the access or release.

Private data provided to the individual must also include the name of the law enforcement agency that submitted the data to CIBRS and the name, telephone number and address of the agency responsible for the data.

A person who is the subject of private data may challenge the data. The Records Supervisor shall review the challenge and determine whether the data should be completed, corrected or destroyed. The corrected data must be submitted to CIBRS and any future dissemination must be of the corrected data.

The Records Supervisor must notify BCA as soon as reasonably practicable whenever data held by CIBRS is challenged. The notification must identify the data that was challenged and the subject of the data.

806.6 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.

806.6.1 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).

806.7 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.

806.8 SECURITY BREACHES

In the event of an actual or potential breach of the security or other unauthorized acquisition of private or confidential information, the Sheriff or designee shall ensure an investigation into the breach is made. Upon completion of the investigation and final disposition of any disciplinary action, a report containing the facts and result of the investigation shall be prepared. If the breach was conducted by an employee, contractor or agent of Beltrami, the report must include a description of the type of data that was breached, the number of individuals whose information was breached, the disposition of any related disciplinary action, and the identity of the employee determined to be responsible for the breach (Minn. Stat. § 13.055).

Written notice shall be given to any individual whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person as soon as reasonably practicable. The notice shall include the following (Minn. Stat. § 13.055):

(a) Notification that an investigation will be conducted.

(b) Notification that a report containing the facts and results will be prepared.

(c) Information on how the person may obtain access to the report, including that he/she may request delivery of the report by mail or email.

The notice may be delayed only so long as necessary to determine the scope of the breach and restore the reasonable security of the data or so long as it will impede an active criminal investigation. Notice shall be made by first class mail, electronic notice or substitute notice as provided in Minn. Stat. § 13.055, Subd. 4. If notification is required to be made to more than 1,000 individuals, notice to all consumer reporting agencies of the timing distribution and content of the notices must also be made (Minn. Stat. § 13.055, Subd. 5).