PUBLIC HEARING

CITY OF BLACKDUCK

Implementation and Purchase a portable recording system for the Blackduck Police Department

Monday, October 28, 2019, @ 6:00pm

AGENDA

1. Convene Meeting / Introductions	Mayor Patch
2. Description of MN Statute §626.8473 subd. 2	Christina Regas, City Admin
3. Policy(s) Review: Portable Audio / Video Recorders Records Maintenance and Release Protected Information Policy	Jace Grangruth, Blackduck P Christina Regas, City Admin
4. General Question and Answer	Jace Grangruth, Blackduck P
5. Adjourn Public Hearing	Mayor Patch

626.8473 PORTABLE RECORDING SYSTEMS ADOPTION; WRITTEN POLICY REQUIRED.

Subdivision 1. **Definition.** As used in this section, "portable recording system" has the meaning provided in section 13.825, subdivision 1.

Subd. 2. **Public comment.** A local law enforcement agency must provide an opportunity for public comment before it purchases or implements a portable recording system. At a minimum, the agency must accept public comments submitted electronically or by mail, and the governing body with jurisdiction over the budget of the law enforcement agency must provide an opportunity for public comment at a regularly scheduled meeting.

Subd. 3. **Written policies and procedures required.** (a) The chief officer of every state and local law enforcement agency that uses or proposes to use a portable recording system must establish and enforce a written policy governing its use. In developing and adopting the policy, the law enforcement agency must provide for public comment and input as provided in subdivision 2. Use of a portable recording system without adoption of a written policy meeting the requirements of this section is prohibited. The written policy must be posted on the agency's website, if the agency has a website.

(b) At a minimum, the written policy must incorporate the following:

(1) the requirements of section 13.825 and other data classifications, access procedures, retention policies, and data security safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;

(2) procedures for testing the portable recording system to ensure adequate functioning;

(3) procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;

(4) circumstances under which recording is mandatory, prohibited, or at the discretion of the officer using the system;

(5) circumstances under which a data subject must be given notice of a recording;

(6) circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;

(7) procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and

(8) procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

History: *2016 c 171 s 6*

PORTABLE AUDIO / VIDEO RECORDERS

PURPOSE AND SCOPE

This policy provides guidelines for the use of portable audio/video recording devices by members of this office while in the performance of their duties (Minn. Stat. § 626.8473). Portable audio /video recording devices include all recording systems whether body-worn, handheld or integrated into portable equipment.

This policy does not apply to mobile audio/video recordings, interviews or interrogations conducted at any City of Blackduck law enforcement, undercover operations, wiretaps or eavesdropping (concealed listening devices) unless captured by a portable recording system.

DEFINITIONS

Definitions related to this policy include:

Portable recording system – A device worn by a member that is capable of both video and audio recording of the member's activities and interactions with others or collecting digital multimedia evidence as part of an investigation and as provided in Minn. Stat. § 13.825.

POLICY

The Blackduck Police Department may provide members with access to portable recorders for use during the performance of their duties. The use of recorders is intended to enhance the mission of the department by accurately capturing contacts between members of the department and the public.

MEMBER PRIVACY EXPECTATION

All recordings made by members on any department issued device at any time or while acting in an official capacity of the department, regardless of ownership of the device, shall remain the property of the department. Members shall have no expectation of privacy or ownership interest in the content of these recordings.

MEMBER RESPONSIBILITIES

Prior to going into service, each uniformed member will be responsible for making sure that he / she is equipped with a portable recorder issued by the department, and that the recorder is in good working order (Minn. Stat § 13.825). If the recorder is not in working order or the member becomes aware of a malfunction at any time, the member shall promptly report the failure to his / her supervisor and obtain a functioning device as soon as reasonably practicable. Uniformed members shall wear the recorder in a conspicuous manner or otherwise notify persons that they are being recorded, whenever reasonably practicable. (Minn. Stat. § 626.8473).

Any member assigned to a non-uniformed position may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable.

When using a portable recorder, the assigned member shall record his / her name, employee number and the current date and time at the beginning and the end of the shift or other period of use, regardless of whether any activity was recorded. This procedure is not required when the recording device and related software captures the user's unique identification and the date and time of each recording.

Members should document the existence of a recording in any report or other official record of the contact, including any instance where the recorder malfunctioned or the member deactivated the recording (Minn. Stat. § 626.8473). Members should include the reason for deactivation.

ACTIVATION OF THE AUDIO / VIDEO RECORDER

This policy is not intended to describe every possible situation in which the recorder should be used, although there are many situations where its use is appropriate. Members should activate the recorder any time the member believes it would be appropriate or valuable to record an incident.

The recorder should be activated in any of the following situations:

a) All enforcement and investigative contacts including stops and field interview (FI) situations

b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.

c) Self-initiated activity in which a member would normally notify the Communication Center.

d) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording.

Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonable appears to the member that such privacy may outweigh any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered using this same criterion. Recording should resume when privacy is no longer at issue unless the circumstances no longer fit the criteria for recording.

At no time is a member expected to jeopardize his / her safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations described above as soon as reasonably practicable.

CESSATION OF RECORDING

Once activated, the portable recorder should remain on continuously until the member reasonably believes that his / her direct participation in the incident is complete or the situation no longer fits the criteria for activation. Recording may be stopped during significant periods of inactivity such as report writing or other breaks from direct participation in the incident. When ceasing the recording, the officer shall narrate the intent and reason, if applicable, then ending the recording.

SURREPTITIOUS RECORDINGS

Minnesota law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his / her permission. (Minn. Stat. §626A.02)

Members of the department may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Chief of Police or the authorized designee.

EXPLOSIVE DEVICE

Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where any explosive device may be present.

IDENTIFICATION AND PRESERVATION OF RECORDINGS

To assist with identifying and preserving data and recordings, members should download, tag or mark the recordings in accordance with procedure and document the existence of the recording in any related case report.

A member should transfer, tag or mark recordings when the member believes:

a) The recording contains evidence relevant to potential criminal, civil or administrative matters.

b) A complainant, victim or witness has requested non-disclosure.

c) A complainant, victim or witness has not requested non-disclosure but the disclosure of the recording may endanger the person.

d) Disclosure may be an unreasonable violation of someone's privacy.

e) Medical or mental health information is contained.

f) Disclosure may compromise an under-cover officer or confidential informant.

g) The recording or portions of the recording may be protected under the Minnesota Data Practices Act.

Any time a member reasonably believes a recorded contact may be beneficial in a non-criminal matter (e.g. a hostile contact), the member should promptly notify a supervisor of the existence of the recording.

REVIEW OF RECORDED MEDIA FILES

When preparing written reports, members should review their recordings as a resource (See the Officer-Involved Shootings and Deaths Policy for guidance in those cases.). However, members shall not retain personal copies of recordings. Members should not use the fact that a recording was made as a reason to write a less detailed report.

Supervisors are authorized to review relevant recordings any time they are investigating alleged misconduct or reports of meritorious conduct or whenever such recordings would be beneficial in reviewing the member's performance.

Recorded files may also be reviewed:

a) Upon approval by a supervisor, by any member of the department who is participating in an official investigation, such as a personnel complaint, administrative investigation or criminal investigation.

b) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.

c) In compliance with the Minnesota Data Practices Act requests, if permitted or required by the Act, including pursuant of Minn. Stat. § 13.82, Subd. 15, and in accordance with the Records Maintenance and Release Policy.

All recordings should be reviewed by the Custodian of Records prior to public release (See the Records Maintenance and Release Policy). Recordings that are clearly offensive to common sensibilities should not be publicly released unless disclosure is required by law or order of the court (Minn. Stat. § 13.82, Subd. 7; Minn. Stat. § 13.825, Subd. 2).

COORDINATOR

The Chief of Police or the authorized designee should designate a coordinator responsible for (Minn. Stat. § 626.8473; Minn. Stat. § 13.825):

a. Establishing procedures for the security, storage and maintenance of data and recordings.

1. The coordinator shall work with the Custodian of Records and the member assigned to coordinate the use, access and release of protected information to ensure that procedures comply with requirements of the Minnesota Government Data Practices Act (MGDPA) and other applicable laws (Minn. Stat. § 13.01 et seq.) (See the Protected Information and the Records Maintenance and Release policies)

b. Establishing procedures for accessing data and recordings.

   1. These procedures should include the process to obtain written authorization for access to non-public data by City of Blackduck members and members of other governmental entities and agencies.

c. Establishing procedures for logging and auditing access.

d. Establishing procedures for transferring, downloading, tagging or marking events.

e. Establishing an inventory of portable recorders including:

   1. Total number of devices owned or maintained by the Blackduck Police Department.

   2. Daily record of the total number of deployed and used by members and, if applicable, the precinct or district in which the devices were used.

   3. Total amount of recorded audio and video data collected by the devices and maintained by the Blackduck Police Department.

f. Preparing the biennial audit required by Minn. Stat. § 13.825 Subd. 9.

g. Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the Blackduck Police Department that expands the type of scope of surveillance capabilities of the department's portable recorders.

PROHIBITED USE OF AUDIO / VIDEO RECORDERS

Members are prohibited from using office-issued recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on-duty or while acting in their official capacity.

Members are also prohibited from retaining recordings of activities of information obtained while on-duty, whether the recording was created with office-issued or personally owned recorders. Members shall not duplicate or distribute such recordings, except for authorized legitimate office business purposes. All such recordings shall be maintained at the department.

Members are prohibited from using personally owned recording devices while on-duty without the express consent of the Chief of Police or designee. Any member who uses a personally owned recorder for office-related activities shall comply with the provisions of this policy, including retention and release requirements and should notify the on-duty supervisor of such use as soon as reasonably practicable.

Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

RETENTION OF RECORDS

All recordings shall be retained for a period consistent with the requirements of the organization's records retention schedule but in no event for a period less than 90 days.

If an individual captured on a recording submits a written request, the recording may be retained for an additional time period. The coordinator should be responsible for notifying the individual prior to destruction of the recording. (Minn. Stat. § 13.825).

RELEASE OF AUDIO / VIDEO RECORDINGS

Requests for the release of audio / video recordings shall be processed in accordance with the Records Maintenance and Release Policy.

ACCESS TO RECORDINGS

Except as provided in Minn. Stat. § 13.825, Subd. 2, audio / video recordings are considered private or nonpublic data.

Any person captured in a recording may have access to the recording. If the individual requests a copy of the recording and does not have the consent of other non-law enforcement individuals captured on the recording, the identity of those individuals must be blurred or obscured sufficiently to render the subject unidentifiable prior to release. The identity of on-duty peace officers may not be obscured unless their identity is protected under Minn. Stat. § 13.82, Subd. 17.

ACCOUNTABILITY

Any member who accesses or releases recordings without authorization may be subject to discipline. (See the Standards of Conduct and the Protected Information policies) (Minn. Stat. § 626.8473).

Records Maintenance and Release

Purpose and Scope

This policy provides guidance on the maintenance and release of office records. Protected information is separately covered in the Protected Information Policy.

Definitions

Definitions related to this policy include:

Confidential Data on Individuals - Data classified as confidential by state or federal law and that identifies individuals and cannot be disclosed to the public or even to the individual who is the subject of the data (Minn. Stat. §13.02, Subd. 3.)

Corrections and Detention Data – Data on individuals created, collected, used or maintained because of their lawful confinement or detainment in state reformatories, prisons and correctional facilities, municipal or county jails, lockups, work houses, work farms and all other correctional and detention facilities (Minn. Stat. § 13.85, Subd 1).

Data on Individuals – All government data in which any individual is or can be identified as the subject of the data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual (Minn. Stat. § 13.02, Subd. 5).

Government Data - Data collected, created, received, maintained or disseminated by this office regardless of its physical form, storage media or conditions of use (Minn. Stat. § 13.02, Subd 7).

Private Data – Data classified as private by state or federal law and that identifies individuals that are only available to the individual who is the subject of the data or with the individual's consent (Minn. Stat. § 13.02, Subd. 12).

Policy

The Blackduck Police Department is committed to providing public access to records and data in a manner that is consistent with the Minnesota Government Data Practices Act (MGDPA) and Official Records Act (Minn. Stat. § 13.03; Minn. Stat. § 15.17).

Custodian of Records Responsibilities

The Chief of Police shall designate a Custodian of Records. The responsibilities of the Custodian of Records include, but are not limited to:

a. Managing the records management system for the Office, including the retention archiving, release and destruction of office data (Minn. Stat. § 15.17, Minn. Stat. § 138.17, Subd. 7).

b. Maintaining and updating the office records retention schedule including:

   a) Identifying the minimum length of time the Office must keep data.

   b) Identifying the office division responsible for the original data.

c. Establishing rules regarding the inspection and copying of office data as reasonably necessary for protection of such data.

d. Identifying data or portions of data that are confidential under state or federal law and not open for inspection or copying.

e. Establishing rules regarding the processing of subpoenas for production of data.

f. Ensuring a current schedule of fees for public data as allowed by law is available.

g. Ensuring the posting or availability to the public a document that contains the basic rights of a person who requests government data, the responsibilities of the Office and any associated fees (Minn. Stat. § 13.025).

h. Ensuring data created by the Office is inventoried and subject to inspection and release pursuant to lawful requests consistent with the MGDPA requirements (Minn. Stat. § 13.03, Subd. 1).

Processing Requests For Public Records
Any office member who receives a request for data shall route the request to the Custodian of Records or the authorized designee.

Requests for Records
The process for requests of data is subject to the following:

a. A person shall be permitted to inspect and copy public government data upon request at reasonable times and places and shall be informed of the data's meaning if requested (Minn. Stat. § 13.03, Subd. 3).

1. The Office may not charge or require the requested person to pay a fee to inspect data. Inspection includes, but not limited to, the visual inspection of paper and similar types of government data. Inspection does not include printing copies, unless printing a copy is the only method to provide for inspection of the data (Minn. Stat. § 13.03, Subd. 3(b)).

2. For data stored and made available in electronic form via remote access, public inspection includes allowing remote access by the public and the ability to print copies or download the data. A fee may be charged for remote access to data where

either the data or the access is enhanced at the request of the person seeking access (Minn. Stat. § 13.03, Subd. 3(b)).

b. Government data maintained by this office using a computer storage medium shall be provided in that medium in electronic form, if a copy can be reasonably made. The Office is not required to provide the data in an electronic format or program that is different from the format or program in which the data is maintained. (Minn. Stat. § 13.03, Subd. (3 e)).

c. The Office is not required to create records that do not exist.

d. The Custodian of Records or designee processing the request shall determine if the requested data is available and, if so, whether the data is restricted from release or denied. The Custodian of Records or designee shall inform the requesting person of the determination either orally at the time of the request or in writing as soon after that time as reasonably possible. The Custodian of Records or designee shall cite the specific statutory section, temporary classification or specific provision of state or federal law on which the determination is based. Upon the request of any person denied access to data, the denial shall be certified in writing (Minn. Stat. § 13.03, Subd. 3 (f)).

e. When a record contains data with release restrictions and data that is not subject to release restrictions, the restricted data shall be redacted and the unrestricted data released.

1. A copy of the redacted release should be maintained in the case file for proof of what was actually released and as a place to document the reasons for the redactions. If the record is audio or video, a copy of the redacted audio/video release should be maintained in the office-approved media storage system and a notation should be made in the case file to document the release and the reasons for the redacted portions.

Release Restrictions

Example of release restrictions include:

a) Personal identifying information, including an individual's photograph; Social Security and driver identification numbers; name, address and telephone number; a medical or disability information that is contained in any driver's license records, motor vehicle authorized by the Office, and only when such use or disclosure is permitted or required by law to carry out a legitimate law enforcement purpose (18 USC § 2721; 18 USC § 2722).

b) Private data on the following individuals (Minn. Stat. § 13.82, Subd. 17).

1. An undercover law enforcement officer.
2. A victim or alleged victim of criminal sexual conduct, or sex trafficking, or of a violation of Minn. Stat. § 617.246, Subd. 2).
3. A paid or unpaid informant if the Office reasonably believes revealing the identity would threaten the personal safety of the informant.

4. A victim of or witness to a crime or if the victim or witness specifically requests not to be identified publicly, unless the office reasonably determines that revealing the identity of the victim or witness would not threaten the personal safety or property of the individual.
5. A person who placed a call to a 9-1-1 system or identity of the person whose phone was used to place a call to the 9-1-1 system when revealing the identity may threaten the personal safety or property of any person or the purpose of the call was to receive help in a mental health emergency. A voice recording of a call placed to the 9-1-1 system is deemed to reveal the identity of the caller.
6. A juvenile witness when the subject matter of the investigation justifies protecting the identity of the witness.
7. A mandated reporter.

c. Audio recordings of calls placed to a 9-1-1 system requesting law enforcement, fire or medical agency response, except that a written transcript of the call is public unless it reveals the identity of protected individuals. (Minn. Stat. § 13.82, Subd. 4).

d. Criminal investigation data involving active cases and inactive investigation data (Minn. Stat. § 13.82, Subd. 7):

1. If the release of the data would jeopardize another ongoing investigation or would reveal the identity of protected individuals or is otherwise restricted.
2. Images or recordings, including photographs, video and audio records that are clearly offensive to common sensibilities. However, the existence of any such image or recording shall be disclosed.
3. As otherwise restricted by law.

e. Juvenile records a data (Minn. Stat. § 260B.171).

f. State criminal history data held in the Bureau of Criminal Apprehension (BCA) database including, but not limited to, fingerprints, photographs, identification data, arrest data, prosecution data, criminal court data, custody and supervision data (Minn. Stat. § 13.87).

g. Traffic collision reports and related supplemental information (Minn. Stat. § 169.09, Subd. 13).

h. Corrections and detention data (Minn. Stat. § 13.85).

i. Personnel data except, unless otherwise restricted, (Minn. Stat. § 13.43, Subd. 2):

1. Name, employee identification number and some aspects of compensation.
2. Job title, bargaining unit, job description, education and training background and previous work experience.
3. Date of first and last employment.
4. Existence and status of any complaints or charges against the employee, regardless of whether the complaint or charge resulted in a disciplinary action.

5. Final disposition of any disciplinary action together with the specific reasons for the action, and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of this office.
6. Terms of any agreement settling any dispute arising out of an employment relationship.
7. Work location, work telephone number, badge number and honors and awards received.
8. Time sheets or other comparable data only used to account for an employee's work time for payroll purposes, excluding the use of sick or other medical leave or other nonpublic data.
9. All other personal data regarding employees of this office are private data and may only be released as authorized by that classification.

j. Any data that was created under the direction of authority of the County Attorney exclusively in anticipation of potential litigation involving this office shall be classified as protected nonpublic or confidential data while such action is pending (Minn. Stat. § 13.39).

k. All data collected by an Automated License Plate Reader (ALPR) on individuals or nonpublic data absent an exception (Minn. Stat. § 13.82; Min Stat §13.824).

l. Response or incident data, so long as the Custodian of Records determines that public access would likely endanger the physical safety of an individual or cause a perpetrator to flee, evade detection or destroy evidence (Minn. Stat. § 13.82, Subd. 14).

Any other record not addressed in this policy shall not be subject to release where such record is classified as other than public data. All public data shall be released as required by the MGDPA (Minn. Stat. § 13.01, Subd. 1).

Subpoenas and Discover Requests
Any member who receives a subpoena duces tecum or discovery request for data should promptly contact a supervisor and the Custodian of Records for review and processing. While a subpoena duces tecum may ultimately be subject to compliance, it is not an order from the court that will automatically require the release of the requested data.

Generally, discovery requests and subpoenas from criminal defendants and their authorized representatives (including attorneys) should be referred to the County Attorney or the courts.

All questions regarding compliance with any subpoena duces tecum or discovery request should be promptly referred to legal counsel for the Office so that a timely response can be prepared.

Release Records to Be Marked
Each page of any written record released pursuant to this policy should be stamped in a colored ink or otherwise marked to indicate the office name and to whom the record was released.

Each audio / video recording released shall include the office name and to whom the record was released.

Expungement
A petition for expungement and expungement orders received by the Office shall be reviewed for appropriate action by the Custodian of Records.

Orders of Expungement
The Custodian of Records shall expunge such records as ordered by the court. Records may include, but are not limited to, a record of arrest, investigation, detention or conviction. Once a record is expunged, members shall respond to any inquiry as though the record did not exist.

Upon request by the individual whose records are to be expunged, the Custodian of Records must send a letter at an address provided by the individual confirming the receipt of the expungement order and that the record has been expunged (Minn. Stat. § 609A.03, Subd. 8).

Expunged records may be opened only by court order (Minn. Stat. § 609A.03, Subd. 7).

Expunged records of conviction may be opened for purposes of evaluating a prospective employee of the Office without a court order.

The Custodian Records shall inform any law enforcement, prosecution or corrections authority, upon request, of the existence of a sealed record and of the right to obtain access to it.

Petition for Expungement
When responding to a petition for expungement, the Custodian of Records shall inform the court and the individual seeking expungement that the response contains private or confidential data (Minn. Stat. § 609A.03, Subd. 3).

Maintenance of Closed Records
Records such as offense reports, arrest reports, juvenile records or other sensitive records shall be secured in such a manner as to reasonably protect them from unauthorized disclosure. Closed records shall be kept separately from public records and shall remain confidential.

Protected Information

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 Blackduck Police Department. 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.

Definitions

Definitions related to this policy include:

Protected information – Any information or data that is collected, stored or accessed by members 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.

Policy

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

Responsibilities

The Chief of Police 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 maintain 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 requirement 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 Blackduck Police Department 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).

Access to Protected Information

Protected information shall not be accessed in violation of any law, order, regulation, user agreement, Blackduck Police Department 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.

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 reasonable 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.

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)).

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 an 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.

Security of Protected Information

The Chief of Police 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 Beltrami County Sheriff and appropriate authorities.

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).

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.

Security Breaches

In the event of an actual or potential breach of the security or other unauthorized acquisition of private or confidential information, the Chief of Police 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 Blackduck, the report must

include a description of the type of data that was breached, the number of individuals whose information was breached, the deposition 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).