



INDEPENDENT AUDITOR'S REPORT

Blackduck Police Department



APRIL 4TH, 2025
RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Blackduck City Council and Chief Arhart:

We have audited the body-worn camera (BWC) program of the Blackduck Police Department (BPD) for the two-year period ended 5/31/2024. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)¹ program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Blackduck Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On October 7, 2024, Rampart Audit LLC (Rampart) met with Chief Josh Arhart, who provided information about BPD's BWC program policies, procedures and operations. As part of the audit, Rampart reviewed those policies, procedures and operations for compliance with Minnesota Statute §626.8473, which sets forth the requirements for creating and implementing a BWC program, and Minnesota Statute §13.825, which governs the operation of BWC programs. In addition, Rampart also conducted a sampling of BWC data to verify BPD's recordkeeping.

The Beltrami County Sheriff's Office (BCSO) hosts both the records management system (RMS) employed by BPD to record calls for service and cases, and the secure servers on which BPD's BWC data are stored. Rampart has previously reviewed BCSO's BWC data management practices as part of audits of that agency and of Bemidji Police Department, which also utilizes BCSO's BWC data storage system, in October 2023 and February 2024, respectively. In addition, Darby Shegrud of Beltrami County's Information Technology department joined Blackduck Police Department's audit by phone to provide information.

The purpose of this report is to provide an overview of our audit, and to provide recommendations to improve the BPD BWC program and enhance compliance with statutory requirements.

BPD BWC Program Implementation and Authorization

Effective August 1, 2016, Minnesota Statute §626.8473 Subd. 2 requires that:

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.

¹ It should be noted that Minnesota statute uses the broader term "portable recording system" (PRS), which includes body-worn cameras. Because body-worn cameras are the only type of portable recording system employed by BPD, these terms may be used interchangeably in this report.

In addition, §626.8473 Subd. 3(a) requires that the law enforcement agency establish and enforce a written policy governing the use of its portable recording system, and states “[t]he written policy must be posted on the agency’s Web site, if the agency has a Web site.”

Rampart previously audited BPD’s BWC program in 2023. As part of that audit, Chief Arhart provided documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the implementation of BCSO’s BWC program. Specifically, Chief Arhart furnished the following:

1. A “Notice of Public Hearing to Receive Public Comment,” which announced that a public hearing would be held at Blackduck City Hall at 6:00 P.M. on October 28, 2019, “to receive public comment for the Blackduck Police Department to purchase and implement a portable recording system.” The notice indicated that comments could be submitted in writing or electronically before the meeting or in person during the meeting. While no specific directions were provided for submitting written or electronic comments, we noted that Blackduck City Hall’s physical address was listed in the document, and that there was an email address included with the city’s contact information at the bottom of the page.
2. An agenda dated October 28, 2019, for a Public Hearing on the “Implementation and Purchase [of] a portable recording system for the Blackduck Police Department.” The contents of the agenda included: a description of Minn. Stat. §626.8473 Subd. 2; a review of the Portable Audio/Video Recorders policy, the Records Maintenance and Release Policy and the Protected Information policy; and a General Question and Answer session. The agenda also included the text of each of these items.
3. The minutes of the October 28, 2019, Public Hearing, which described information provided during the public hearing, as well as the discussion that followed.

Copies of these documents have been retained in Rampart’s audit files. In our opinion, BPD met the requirements contained in Minn. Stat. §626.8473 Subd. 2 prior to the implementation of its BWC program.

In addition, §626.8473 Subd. 3(a) requires that the law enforcement agency establish and enforce a written policy governing the use of its portable recording system, and states “[t]he written policy must be posted on the agency’s Web site, if the agency has a Web site.”

Rampart verified that there was a working link to BPD’s BWC policy on the Public Safety Page of the City of Blackduck website. In our opinion, Blackduck Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

BPD BWC WRITTEN POLICY

As part of this audit, we reviewed BPD’s BWC policy, a copy of which is attached to this report as Appendix A.

Minnesota Statute §626.8473 Subd. 3(b) requires a written BWC policy to incorporate the following, at a minimum:

1. The requirements of section 13.825 and other data classifications, access procedures, retention policies, and data safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;
2. A prohibition on altering, erasing or destroying any recording made with a peace officer’s portable recording system or data and metadata related to the recording prior the expiration of the applicable

retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely;

3. A mandate that a portable recording system be worn at or above the mid-line of the waist in a position that maximizes the recording system's capacity to record video footage of the officer's activities;
4. A mandate that officers assigned a portable recording system wear and operate the system in compliance with the agency's policy adopted under this section while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official;
5. A mandate that, notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the deceased individual's next of kin, the legal representative of the deceased individual's next of kin, and the other parent of the deceased individual's child, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, with the following exception:
 - A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to section 13.82 subdivision 7;
6. A mandate that, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82 subdivision 7;
7. Procedures for testing the portable recording system to ensure adequate functioning;
8. 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;
9. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
10. Circumstances under which a data subject must be given notice of a recording;
11. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
12. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
13. 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.

In our opinion, the BPD BWC policy is compliant with respect to clauses 7 – 11.

Due to their complexity and interrelatedness, clauses 1 and 12 are discussed separately below. Clause 13 is also discussed separately.

Clauses 2 – 6 are newly added as a result of 2023 legislation and will also be discussed separately below.

BPD BWC Data Retention

Minn. Stat. §13.825 Subd. 3(a) establishes a minimum retention period of 90 days for all BWC data not subject to a longer retention period, while §13.825 Subd. 3(b) requires that the following categories of BWC data be retained for a minimum period of one year:

- 1) any reportable firearms discharge;
- 2) any use of force by an officer that results in substantial bodily harm; and
- 3) any incident that results in a formal complaint against an officer.

Meanwhile, Subd. 3(c) requires that any portable recording system data documenting a peace officer's use of deadly force must be maintained indefinitely. Finally, Subd. 3(d) requires that an agency retain BWC recordings for an additional period of up to 180 days when so requested in writing by a data subject.

The Retention of Records section of BPD's BWC policy states that "[a]ll recordings shall be maintained 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." BPD's BWC policy includes the agency's retention schedule.

BPD's BWC policy includes the data categories enumerated in §13.825 Subd. 3(b) and (c), but fails to assign a retention period for them. Chief Arhart indicated that the retention schedule in place in the video management software reflects the correct retention periods for these data types, but that this information was inadvertently omitted from the written policy.

BPD's policy addresses the §13.825 Subd. 3(d) requirement, and notes that such additional retention is mandatory.

Prior to the issuance of this report, BPD submitted a revised BWC policy that includes the required retention periods specified in Subdivision 3(b) and (c). The revised policy is attached to this report as Appendix B. In our opinion, this revised policy meets the retention requirements contained in Minn. Stat. §13.825 Subd. 3.

BPD's BWC policy does not address the prohibition against altering, erasing or destroying BWC data or metadata prior to the expiration of the scheduled retention period, which is described in Clause 2 of the Policy section of this report. Prior to the issuance of this report, BPD furnished a revised BWC policy that addresses this requirement.

BPD employs Panasonic body-worn cameras. The Beltrami County Sheriff's Office manages BWC data retention on BPD's behalf on their own secure server through automated retention settings in the Panasonic Unified Digital Evidence (UDE) video management software. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be adjusted as needed.

BPD's BWC policy requires that each officer transfer data from his or her body-worn camera to the appropriate server by the end of each shift, and also requires that the officer assign the appropriate label or labels to each file to identify the nature of the data. These labels then determine the appropriate retention period for each file. If an officer fails to label a recording, the retention period is set to permanent to avoid the accidental loss of data.

In our opinion, BPD's revised BWC policy is compliant with respect to applicable data retention requirements.

BPD BWC Data Destruction

BCSO IT Technician Shegrud has previously advised us that BPD BWC data are stored on BCSO-owned servers located on-site at the sheriff's office. These servers are backed-up on a nightly basis through an automated process to guard against unintentional loss of data.

Data on these servers are destroyed through automated deletion and overwriting, based on a retention schedule assigned to each video. In addition, at the time it is retired from service, any BCSO-owned physical hard drive used to store BWC data will have all data deleted prior to being destroyed by physical means, specifically crushing. This is consistent with FBI CJIS policy, which requires that hard drives used for CJIS data storage are sanitized by overwriting at least three times or degaussing prior to being released to unauthorized individuals, while inoperable drives must be destroyed through physical means such as shredding.

In our opinion, BPD's BWC policy is compliant with respect to the applicable data destruction requirements.

BPD BWC Data Access

Any request for access to BWC data by a data subject or member of the media would be made in writing to the Blackduck City Administrator, who would then forward the request to Chief Arhart for review. Approved requests are processed by the Beltrami County Sheriff's Office Records Department, which serves as the Custodian of Records for BPD BWC data. BWC data are typically provided to data subjects via physical media, such as a DVD or USB memory device.

Though not addressed in the BWC policy, Chief Arhart advised us that BPD BWC data are shared with other law enforcement agencies for evidentiary purposes only. All such requests must be made by email to Chief Arhart by the requesting agency's chief law enforcement officer (CLEO). Existing verbal agreements between BPD and other area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b). Access to BPD BWC data for outside agencies is normally provided via optical disc.

Prosecutors contact BCSO Records staff directly when requesting BWC data. Such requests are reviewed by Records staff prior to fulfillment.

We recommend adding language to the BWC policy stating that BWC data will be shared with other agencies only for legitimate law enforcement purposes that are disclosed in writing at the time of the request. We also recommend that BPD obtain a written acknowledgement from each outside law enforcement agency that any BWC data obtained from BPD will be managed by the requesting agency in compliance with the requirements of §13.825 Subd. 7 and 8. A copy of this written acknowledgment should be maintained on file.

Prior to the issuance of this report, BPD submitted a revised BWC policy that addresses these recommendations.

As discussed in Clauses 5 and 6 of the Policy section of this report, the Minnesota State Legislature in 2023 added specific access requirements related to BWC data that document deadly force incidents, and specified that these requirements must be included in the agency's BWC policy. At the time of our audit, BPD had not

addressed these new requirements. Prior to the issuance of this report, BPD submitted a revised BWC policy that added language to meet these requirements.

In our opinion, BPD's revised BWC policy is compliant with respect to the applicable data access requirements.

BPD BWC Data Classification

BPD's BWC policy identifies all BWC data as private or nonpublic, "[e]xcept as provided in Minn. Stat. §13.825 Subd. 2." In our opinion, incorporating by reference the exceptions identified in §13.825 Subd. 2 satisfies the applicable data classification requirements.

BPD BWC Internal Compliance Verification

The Review of Recorded Media Files section of the BPD BWC policy states that "[s]upervisors 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," and also notes that recordings may be reviewed "[b]y a supervisor as part of internal audits and reviews as required by Minn. Stat. §626.8473." This section of the BWC policy also states: "[s]upervisors will periodically conduct spot checks (audits) of officers Body Worn Camera footage and insure (sic) that officers are compliant with this policy."

As discussed in Clause 4 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must require that an officer assigned a BWC wear and operate the system in compliance with the agency's BWC policy while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official.

BPD's BWC policy does not address the requirements discussed in the preceding paragraph. Prior to the issuance of this report, BPD submitted a revised BWC policy that addressed this requirement.

In our opinion, this revised policy language satisfies the requirements of Clause 4.

The Accountability section of the BPD BWC policy states that "[a]ny member who accesses or releases recordings without authorization may be subject to discipline (See the Standards of Conduct and Protected Information policies)." This subsection also references Minn. Stat. §626.8473. The Policy section of the BWC policy contains additional language noting that "[m]embers of the Blackduck Police Department that violate this policy will be subject to progressive discipline." Because certain violations of Minn. Stat. Chapter 13 can be charged as misdemeanors, we recommend that BPD add language noting that violations of the BWC policy may also result in prosecution.

In our opinion, BPD's BWC policy is compliant with respect to the compliance and disciplinary requirements contained in §626.8473 Subd. 3(b)(12).

BPD BWC Program and Inventory

BPD currently possesses two (2) Panasonic iPRO body-worn cameras.

The BPD BWC policy identifies those circumstances in which officers are expected to activate their body-worn cameras, as well as circumstances in which they are prohibited from activating their body-worn cameras. The policy also provides guidance for those circumstances in which BWC activation is deemed discretionary.

The Prohibited Use of Audio/Video Recorders section of the BPD BWC policy states in part that “[m]embers are prohibited from retaining recordings of activities or information obtained while on-duty, whether the recording was created with office-issued or *personally owned recorders* [italics added].”

Minn. Stat. §13.825 Subd. 6, Use of agency-issued portable recording systems, states: “While on duty, a peace officer *may only use a portable recording system issued and maintained by the officer’s agency* [italics added] in documenting the officer’s activities.”

We recommend removing the phrase referencing “personally owned recorders.” While nothing in BPD’s BWC policy authorizes the use of personally-owned recording devices, we also recommend that BPD add language to specifically prohibit the use of such devices.

While BPD does not maintain a separate log of BWC deployment or use, Chief Arhart advised us that because each officer wears a BWC while on duty, the number of BWC units deployed each shift can be determined based on a review of BPD payroll records. Actual BWC use would be determined based on the creation of BWC data.

As of the date of the audit, BPD maintained 300 BWC data files.

BPD BWC Physical, Technological and Procedural Safeguards

BPD BWC data are initially recorded to an internal hard drive in each officer’s BWC. Those files are then transferred to the dedicated BWC servers at the Beltrami County Sheriff’s Office by means of a physical docking station utilizing a wired connection to the BCSO servers. The BCSO servers are secured behind multiple locked doors. As noted earlier in this report, BCSO employs multiple servers to guard against possible loss of data due to a hardware failure.

Chief Arhart advised that BPD recently purchased a new squad that is capable of uploading BWC data wirelessly to the BCSO servers.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes through the Panasonic UDE software.

BPD’s BWC policy states that: “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.” In addition: “Members are also prohibited from retaining recordings of activities of [sic] information obtained while on duty...”

As noted above, requests by other law enforcement agencies for BPD BWC data must be approved by Chief Arhart and are fulfilled via optical disc. A similar method is employed to submit BPD BWC data to the Beltrami County Attorney’s Office.

The Member Responsibilities section of BPD's BWC policy states: "Uniformed members shall wear the recorder in a conspicuous manner or otherwise notify persons that they are being recorded, whenever reasonably practicable." As discussed in Clause 3 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must specify that a BWC be worn at or above the mid-line of the waist. Prior to the issuance of this report, BPD submitted a revised BWC policy that addresses this requirement. On review, we noted that in the paragraph following the updated language, we found old language that appears to be a relic of the old policy stating "non-uniformed members should wear the recorder in a conspicuous manner when in use." As there is no exception regarding the statutory mandate as noted above with regards to the mid-line of the waist mandate, Rampart recommends removing this line from the updated policy to avoid confusion and replace it with "all peace officers" versus uniformed or non-uniformed. In our opinion, this revised BWC policy satisfies this requirement.

Enhanced Surveillance Technology

BPD currently employs BWCs with only standard audio/video recording capabilities. They have no plans at this time to add enhanced BWC surveillance capabilities, such as thermal or night vision, or to otherwise expand the type or scope of their BWC technology.

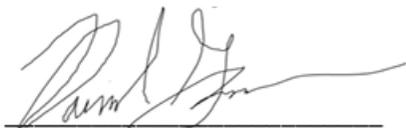
If BPD should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses.

Data Sampling

Rampart selected a random sample of 132 calls for service (CFS) from which to review any available BWC recordings. It should be noted that not every call will result in an officer activating his or her BWC. For example, an officer who responds to a driving complaint but is unable to locate the suspect vehicle would be unlikely to activate his or her BWC. It should also be noted that because the audit covers a period of two years, while most BWC data is only required to be retained for 90 days, there is a significant likelihood that the sample population will include ICRs for which BWC data was created, but which has since been deleted due to the expiration of the retention period.

Audit Conclusions

In our opinion, the Blackduck Police Department's Body-Worn Camera Program and revised BWC policy are substantially compliant with Minnesota Statutes §13.825 and §626.8473.

A handwritten signature in black ink, appearing to read "Rampart Audit", is written over a solid horizontal line.

Rampart Audit LLC

4/04/2025

APPENDIX A:

City of Blackduck Police Department Portable Audio / Video Recorders

Adopted: October 7, 2019

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).

APPENDIX B:

City of Blackduck Police Department

Portable Audio / Video Recorders

Adopted: October 7, 2019 Updated: January 6, 2025

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. Members of the Blackduck Police Department that violate this policy will be subject to progressive discipline.

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 they are equipped with a portable recorder issued by the department, and that the recorder is in good working order (Minn. Stat § 13.825). At the beginning of a member’s shift, they will turn on the portable recorder and insure it turns on, boots up, goes into standby mode, and is capable of being activated to initiate a recording. Officers will periodically check to insure the device is recording and offloading to the portable recorder server. 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 their supervisor and obtain a functioning device as soon as reasonably practicable. **Uniformed officers must position body worn cameras at or above mid-line of the waist in a position that maximized the recording system's capacity to record video footage of the officer's activities 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 their 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.

Officers of the Blackduck Police Department shall follow this agency's body worn camera policy when acting under the command and control of another Chief Law Enforcement Officer or Federal Law Enforcement Official.

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.

Rampart Audit, LLC

Officers will not activate or record with a portable recording device in the Beltrami County Jail Control Rooms or Administrative offices.

At no time is a member expected to jeopardize their 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 their 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 their 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.

Rampart Audit, LLC

- 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.

Supervisors will periodically conduct spot checks (audits) of officers Body Worn Camera footage and insure that officers are compliant with this policy.

Recorded files may also be reviewed:

- a) By a supervisor as part of internal audits and reviews as required by Minn. Statute §626.8473.
- b) 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.
- c) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.
- d) By media personnel with permission of the Chief of Police or the authorized designee.
- e) 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

Rampart Audit, LLC

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 Custodian of Records shall be Beltrami County Sheriff Office.
 2. 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)
 3. The coordinator should work with the Custodian of Records to identify recordings that must be retained for a specific time frame under Minnesota Law (e.g. firearm discharges, certain use of force incidents, formal complaints).
- 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.
- h. Ensuring that this Portable Audio/Video Recorders Policy is posted on the City of Blackduck website.

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.

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.

The following retention periods apply to the following recorded video event descriptions before the videos are purged from the system whether it is the network server or evidence room.

Event Description Retention Period:

<u>Description</u>	<u>Period:</u>
1. Junk	90 days
2. Traffic Stop Warning	90 days
3. Traffic Stop Citation	90 days
4. DWI	365 days
5. Pursuit	365 days
6. Arrest	Until Case is resolved
7. Accident	90 days
8. Audio domestic	365 days
9. Homicide/Sex Assault	Forever
10. Evidence	Until Case is resolved
11. Medical	90 days
12. Statutory	6 years

In addition to the above retention periods, the following will be retained for **one year**.

1. Data that documents the use of a sufficient type or degree to require a use of force report or supervisory review including the use of force by an officer that results in substantial bodily harm.
2. Data that documents a **reportable** discharge of a firearm by an officer in the course of their duties.

3. Data documenting circumstances that have given rise to a formal complaint against an officer.

Any body worn camera recording, including related data or metadata, documenting an officer's use of deadly force shall be maintained indefinitely.

No data including data or metadata, shall be altered, erased, or destroyed prior to the expiration of the applicable retention period.

Upon written request by a BWC and SCVC data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days.

The agency will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received.

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. BWC video shall be shared with other agencies only for legitimate law enforcement purposes that are documented in writing at the time of the request. A copy of all written requests shall be retained on file.

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.

When an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the following individuals, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, except as otherwise provided in this clause:

1. the deceased individual's next of kin;
2. the legal representative of the deceased individual's next of kin; and

3. the other parent of the deceased individual's child.

A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to MN Statute 626.8473 Section 13.82, subdivision 7.

When an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than what is required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by MN Statute 626.8473 Section 13.82, subdivision 7.

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).

Any person who willfully violates the provisions of this policy or any rules adopted under this policy or whose conduct constitutes the knowing unauthorized acquisition of not public data, as defined in Minn. Statute Section 626.8473 13.055, subdivision 1, is guilty of a misdemeanor.

Willful violation of this policy, including any action subject to a criminal penalty noted above, by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.