



INDEPENDENT AUDITOR'S REPORT

Lamberton Police Department



AUGUST 8TH, 2026
RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Lamberton City Council and Chief Determan:

We have audited the body-worn camera (BWC) program of the Lamberton Police Department (LPD) for the two-year period ended 5/13/2026. 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 Lamberton Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On June 12, 2026, Rampart Audit, LLC (Rampart) met with Chief Derick Determan, who provided information about LPD'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 LPD's recordkeeping.

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

LPD 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.

Chief Determan provided the following documentation to verify that Lamberton Police Department had satisfied these requirements prior to the implementation of its BWC program:

- A copy of a public notice providing information about the proposed BWC program, including directions for obtaining a copy of the draft BWC policy to review, as well as the time, date and location of the public hearing, and instructions for submitting written comments via mail or email, or in-person comments during the 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 LPD, these terms may be used interchangeably in this report.

- A copy of the June 10, 2024, Lamberton City Council meeting minutes, noting that the council voted unanimously to approve the proposed BWC policy following the public hearing held the previous month.

In addition, Rampart located a copy of the May 13, 2024, Lamberton City Council meeting minutes, which documented that a public hearing was held for the purpose of receiving comments regarding the proposed BWC program and policy. Copies of these documents have been retained in our audit files. In our opinion, LPD satisfied the requirements of §626.8473 Subd. 2 prior to the implementation of its BWC program.

Minn. Stat. §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.”

Chief Determan provided a copy of LPD’s written BWC policy and Rampart verified that the policy was accessible on the Lamberton Police Department webpage.

In our opinion, Lamberton Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

LPD BWC WRITTEN POLICY

As part of this audit, we reviewed LPD’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) 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 LPD 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.

LPD 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 Recordings section of Lamberton Police Department's BWC policy states that: "[a]ll 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," which satisfies the requirements of §13.825 Subd. 3(a).

The Portable Audio/Video Recorder Retention Requirements section of the policy identifies a retention period of one year for reportable firearms discharges, six years for incidents involving the use of force by a law enforcement officer and six years for incidents resulting in an administrative complaint against an officer. In our opinion, this satisfies the requirements of §13.825 Subd. 3(b).

The Portable Audio/Video Recorder Retention Requirements section of the policy identifies the retention period as "Indefinite/Permanent" for "an incident involving the use of deadly force by an officer of this department or another agency." In our opinion, this satisfies the requirements of §13.825 Subd. 3(c).

The Retention of Recordings section of Lamberton Police Department's BWC policy addresses the §13.825 Subd. 3(d) requirement pertaining to additional retention when so requested by a data subject.

In our opinion, Lamberton PD's BWC policy meets or exceeds the retention requirements contained in Minn. Stat. §13.825 Subd. 3.

As discussed in Clause 2 of the Policy section of this report, the Accountability section of LPD's BWC policy states that "[a]ny member who alters or destroys BWC video or associated data and metadata prior to its expiration period outlined in the retention schedule may be subject to discipline and or criminal consequences."

Chief Determan advised us that LPD retired its previous Watchguard body-worn camera in March of 2026 and replaced it with two (2) Axon 4 BWCs, though the Watchguard BWC is still functional and available as a backup if needed. The Axon BWCs utilize the Axon Evidence (also known as Evidence.com) cloud-based storage and data management systems. BWC data retention is managed through automated retention settings. 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 by Chief Determan as needed. In the event an officer fails to assign a data classification, the default retention period is permanent to avoid the accidental loss of data.

LPD maintains an in-house server to store recordings created by the now-retired Watchguard camera. LPD uses Watchguard Evidence Library software to manage BWC data retention through automated retention settings, following a similar process as the Axon system.

LPD's BWC policy states: "[t]o assist with identifying and preserving data and recordings, member should download, tag, or mark the recordings in accordance with procedure and document the existence of the recording in any related case report."

Chief Determan advised us that the Axon body-worn cameras utilize a physical docking station located at the Lamberton Police Department.

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

LPD BWC Data Destruction

As discussed above, LPD utilizes an in-house server for data storage for its previous BWC system, as well as cloud-based storage for its current system, with retention periods for both determined based on the classification assigned to BWC data. Chief Determan advised us that videos are deleted automatically upon expiration of the assigned retention period.

FBI CJIS policy requires that hard drives used for CJIS data storage be 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.

Chief Determan advised us that any hard drive containing BWC data would be overwritten, erased and physically destroyed once retired from service.

Axon certifies that its cloud service is compliant with the FBI's Criminal Justice Information System Security Division Policy as required by Minnesota Statute §13.825 Subd. 11(b). Data destruction is achieved through automated deletion and overwriting, with storage devices sanitized (overwritten three or more times or degaussed) or physically destroyed upon being removed from service.

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

LPD BWC Data Access

The Access to BWC data by non-employees section of LPD's BWC policy states that:

Officers shall refer members of the media or public seeking access to BWC data to (the responsible authority/data practices designee), who shall process the request in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws.

Chief Determan advised us that that all requests for BWC data from the public or media are made in writing, using Lamberton Police Department's Body Worn Camera Video Request form. Requests are submitted to the City of Lamberton Records Administrator. Chief Determan reviews each request and, if approved, processes and fulfills it. BWC video is provided to members of the public or media via email link, or through physical media such as DVD or USB memory device.

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. These elements are addressed in the Death Resulting From Force – Release of Public Data section of the policy.

The Access to BWC data by non-employees section of LPD's BWC policy states that "BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure. All written requests shall be made through the requestor's government email." In addition, "BWC data shall be made available to prosecutors, courts,

and other criminal justice entities as provided by law.” Chief Determan advised us that such requests are submitted to him via email, and can be fulfilled using Axon Evidence’s internet sharing function, or through physical media if requested. Prosecutors and probation personnel follow the same procedure as other law enforcement personnel to request BWC data.

Chief Determan provided a copy of the BWC video request form, which requires that the requesting officer provide a signed acknowledgment of the receiving agency’s obligations under §13.825 Subd. 7 and 8, which include a requirement to maintain BWC data security.

In our opinion, LPD’s BWC policy is compliant with respect to the applicable data access requirements.

LPD BWC Data Classification

The Access to Recordings section of Lamberton PD’s BWC policy states that “BWC data is presumptively private.” The policy further states that “BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently.” Active criminal investigation data are classified as confidential. LPD’s BWC policy also identifies certain categories of BWC data that are public.

As noted in the preceding section, Lamberton PD’s BWC policy incorporates the changes the Minnesota State Legislature made in 2023 regarding BWC data documenting incidents involving the use of deadly force, including the requirement that, subject to limited redaction and certain exceptions, such BWC data be released to the public no later than 14 days after the incident.

In our opinion, LPD’s BWC policy is compliant with respect to the applicable data classification requirements.

LPD BWC Internal Compliance Verification

The LPD BWC Review of Recorded Media Files section states that recorded files may be reviewed “[b]y a supervisor as part of internal audits and reviews as required by Minn. Stat. § 626.8473,” while the Accountability section states that:

The CLEO or designee will review BWC recordings of each recording device/officer randomly on a weekly basis. The [CLEO] or designee will randomly audit the history of the BWC files to ensure no unauthorized downloading or viewing took place. In the event of a violation, the violator will be disciplined in accordance with department policy.

[a]t least once a month or as soon as practicable, the Police Chief will randomly review BWC usage by each full-time officer or part-time officer that has worked in the previous month to ensure compliance with this policy.” Chief Determan advised that he conducts such reviews as required by the policy, but that there is no formal documentation process. Rampart recommends that such reviews be documented, whether within the video management software itself or through other means.

The Access by peace officers and law enforcement employees section of the BWC policy states that: “[n]o employee may have access to the Department’s BWC data except for legitimate law enforcement or data administration purposes,” and further states that: “[o]fficers may access and view stored BWC

video only when there is a business need for doing so...” Chief Determan advised us that both the previous Watchguard system and the current Axon system have an audit trail feature that allows him to determine who has viewed a BWC recording.

The Prohibited Use of Audio/Video Recorders section of the BWC policy states that: “[m]embers are prohibited from using personally owned recording devices while on duty.”

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.

These requirements are addressed in the Member Responsibilities section of the BWC policy.

The Accountability section of LPD’s BWC policy addresses consequences associated with violations of the policy, to include both disciplinary action and potential criminal penalties.

In our opinion, LPD’s policy is compliant with respect to the compliance and disciplinary requirements contained in §626.8473 Subd. 3(b)(8).

LPD BWC Program and Inventory

LPD currently possesses two (2) Axon 4 body-worn cameras, one (1) of which is in regular use with the other retained as a spare, as well as one (1) Watchguard body-worn camera, which was retired from service as of March of 2026 but is still available as a spare.

The LPD 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.

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. This requirement is addressed in the Member Responsibilities section of LPD’s BWC policy.

Chief Determan advised us that he is able to determine the number of BWCs currently deployed via the Axon GPS feature, which shows the location of each BWC when it is powered on. This information can be determined after the fact by reviewing the schedule and/or payroll data.

As of June 12, 2026, LPD maintained 191 GB of Watchguard BWC videos and 21.93 GB of Axon BWC videos.

LPD BWC Physical, Technological and Procedural Safeguards

LPD BWC data are initially recorded to a hard drive in each officer's BWC. Data from each BWC is then uploaded to Axon's Evidence.com Cloud Service via a physical docking station located at the Police Department.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes, as well as the ability to add or edit case numbers and titles. Officers also have the ability to view non-restricted videos created by other personnel; however, all BWC data access is logged automatically and available for audit purposes.

Enhanced Surveillance Technology

LPD currently employs BWCs with only standard audio/video recording capabilities. LPD has 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 LPD 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 calls for which BWC data was created, but which has since been deleted due to the expiration of the retention period. The auditor reviewed the retained BWC videos to verify that this data was accurately documented in LPD records.

Audit Conclusions

In our opinion, the Lamberton Police Department's Body-Worn Camera Program is compliant with Minnesota Statutes §13.825 and §626.8473.

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

Rampart Audit, LLC

8/08/2026

APPENDIX A:

Portable Audio/Video Recorders:

PURPOSE AND SCOPE:

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

This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any Lamberton Police Department facility, undercover operations, wiretaps, or eavesdropping (concealed listening devices).

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.

BWC - Body worn camera.

POLICY:

The Lamberton Police Department provides 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.

COORDINATOR:

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

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

1. The coordinator should work with the Chief of Police 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).

2. The coordinator should work with the Chief of Police 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).

- 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 LPD members and members of other governmental entities and agencies.

- Establishing procedures for logging or auditing access.
- Establishing procedures for transferring, downloading, tagging, or marking events.
- Establishing an inventory of portable recorders including:

1. The ability to provide the total number of devices owned or maintained by the Lamberton Police Department.

2. The ability to determine the total amount of recorded audio and video data collected by the devices maintained by the Lamberton Police Department.

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

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

- Notifying the Bureau of Criminal Apprehension (BCA) in a timely manner when new equipment is obtained by the Lamberton Police Department that expands the type or scope of surveillance capabilities of the department's portable recorders.
- Ensuring that this portable Audio/Video Recorders Policy is posted on the Department website.

MEMBER PRIVACY EXPECTATION:

All recordings made by members on any department-issued device at any time or while acting in an official capacity of this 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:

All officers assigned a portable recording system shall wear and operate the system in compliance with the Lamberton Police Department's portable audio/video recorders policy, while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official.

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 should wear the recorder in a conspicuous manner located at or above the mid-line of the waist. (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 located at or above the mid-line of the waist when in use.

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:

- All enforcement and investigative contacts including stops and field interview (FI) situations.
- Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops.
- Self-initiated activity in which a member would normally notify Dispatch.
- 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 reasonably 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 an 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. Recordings may be stopped during periods where the officer is engaged in tactical planning or communication with other officers.

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 an explosive device may be present.

PROHIBITED USE OF AUDIO/VIDEO RECORDERS:

Members are prohibited from using department-issued portable 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 or information obtained while on duty. Members shall not duplicate or distribute such recordings, except for authorized legitimate department business purposes. All such recordings shall be retained at the Department.

Members are prohibited from using personally owned recording devices while on duty.

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

RETENTION OF RECORDINGS:

See attached retention schedule

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.

It shall be a violation of this policy for members of the Lamberton Police Department to alter or destroy BWC video prior to its expiration period as outlined in the retention schedule.

If an individual captured in a recording submits a written request, the recording shall be retained for an additional time period of no less than 180 days. 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 access to recordings section of this policy.

ACCESS TO RECORDINGS:

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

Data Subjects. Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:

- Any person or entity whose image or voice is documented in the data.
- The officer who collected the data.
- Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.

BWC data is presumptively private. BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:

- BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.
- Some BWC data is classified as confidential (See Below)
- Some BWC data is classified as public (See Below)

Confidential data. BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the “private” classification listed above and the “public” classifications listed below.

Public Data. The following BWC data is public:

- Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.
- Data that documents the use of force by a peace officer that results in substantial bodily harm.
- Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted. In addition, any data on undercover officers

must be redacted. Data that documents the final disposition of a disciplinary action against a public employee.

- However, if another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other classification. For instance, data that reveals protected identities under Minn. Stat. 13.82, subd. 17 (e.g., certain victims, witnesses, and others) should not be released even if it would otherwise fit into one of the public categories listed above.

Access to BWC data by non-employees. Officers shall refer members of the media or public seeking access to BWC data to (the responsible authority/data practices designee), who shall process the request in accordance with the MGDPA and other governing laws. In particular:

- An individual shall be provided with access and allowed to review recorded BWC data about him- or herself and other data subjects in the recording, but access shall not be granted:

1. If the data was collected or created as part of an active investigation.

1. Data subjects. Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:

1. Any person or entity whose image or voice is documented in the data.

2. To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn Stat. 13.82 subd. 17.

2. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction.

1. Data on other individuals in the recording who do not consent to the release must be redacted.

2. Data that would identify undercover officers must be redacted.

3. Data on other officers who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.

Access by peace officers and law enforcement employees. No employee may have access to the departments BWC data except for legitimate law enforcement or data administration purposes:

- Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Officers may review video footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident.
- Agency personnel shall document their reasons for accessing stored BWC data in the program audit note file of the specific recording or written log at the time of each access. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.
- Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.

Other authorized disclosures of data. Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat 13.82 Sub 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individual identities that are not public. Protecting against incidental disclosure should involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,

- BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure. All written requests shall be made through the requestor's government email.
- BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law. All requests must be in writing and shall be made through the requestor's government email.

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 reasonably believes:

- The recording contains evidence relevant to potential criminal, civil or administrative matters.
- A complainant, victim or witness has requested non-disclosure.
- 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.
- Medical or mental health information is contained.
- Disclosure may compromise an undercover officer or confidential informant.
- 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:

- By a supervisor as part of internal audits and reviews as required by Minn. Stat. § 626.8473.
- 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.
- Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.

- By media personnel with permission of the Chief of Police or the authorized designee.
- In compliance with the Minnesota Data Practices Act request, if permitted or required by the Act, including pursuant to Minn. Stat. § 13.82, Subd. 15, and in accordance with the Records Maintenance and Release Policy.

All recordings should be reviewed by the Chief of Police or their designee 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).

DEATH RESULTING FROM FORCE – RELEASE OF PUBLIC DATA

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, subject to paragraphs (C) and (D)

- The deceased individuals next of kin;
 - The legal representative of the deceased individuals next of kin; and
 - The other parent of the deceased individuals' child.
1. A law enforcement agency may deny a request to inspect portable recording system data under paragraph (b) if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access under this paragraph, the chief law enforcement officer must provide a prompt, written denial to the individual in paragraph (b) 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.
 2. 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 remains classified by section 13.82, subdivision 7.

ACCOUNTABILITY:

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

Any member who alters or destroys BWC video or associated data and metadata prior to its expiration period outlined in the retention schedule may be subject to discipline and or criminal consequences.

The CLEO or designee will review BWC recordings of each recording device/officer randomly on a weekly basis. The Cleo or designee will randomly audit the history of the BWC files to ensure that no unauthorized downloading or viewing took place. In the event of a violation, the violator will be disciplined in accordance with department policy.

Portable Audio/Video Recorder Retention Requirements

1. **Deadly Force:** The information was obtained as part of an incident involving the use of deadly force by an officer of this department or another agency. (**Indefinite/Permanent**)
2. **Reportable Firearms Discharge:** Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous. This shall include accidental or unintentional discharges as well (**One year**)
3. **Evidence-criminal:** The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision. (**Seven years**)
4. **Homicides:** The information has evidentiary value and is involved in apparent or suspected cases involving suspicious deaths or known homicides. (**Permanent**)
5. **Evidence-force:** Whether or not enforcement action was taken, or an arrest resulted, the event involved the application of force by a Law Enforcement Officer of this or another agency. (**Six years**)
6. **Evidence-property:** Whether or not enforcement action was taken, or an arrest resulted, an officer seized property from an individual or directed an individual to dispossess property. (**One year**)

7. **Evidence-administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer. **(6 years if involved in administrative complaint against officer, 365 days if no complaint.)**

8. **Evidence-other:** The recording has potential evidentiary value for reasons determined by the officer at the time of labeling. **(180 days)**

9. **Training:** The event was such that it may have value for training. **(180 days)**

10. **Not Evidence:** The recording does not contain any of the foregoing categories of information and has no apparent evidentiary value. Recordings of general citizen contacts and unintentionally recorded footage are not evidence. **(180 days)**

11. **Signal Test:** The recording was made for the sole purpose of checking the functionality of the body camera to ensure it meets operational requirements and is ready for shift. **(90 days)**

12. **Mental Health:** The recording contains interactions with those suffering from apparent mental health crisis that does not fall into a category with longer retention period. **(Until manually deleted, 180 days minimum)**

13. **Officer Injury:** Recording contains evidence of an Officer being injured while on duty regardless of if incident could be categorized differently. **(Permanent)**

If incident falls into multiple categories, the appropriate category with the longest retention period shall be selected.