INDEPENDENT AUDITOR'S REPORT

Eden Valley Police Department

MAY 6TH, 2025

RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear City Council and Chief Borscheid:

We have audited the body-worn camera (BWC) program of the Eden Valley Police Department (EVPD) for the two-year period ended 02/20/2025. 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 EVPD. Our responsibility is to express an opinion on the operations of this program based on our audit.

On February 26, 2025, Rampart Audit LLC (Rampart) met with Chief Evan Borscheid, who provided information about EVPD'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 EVPD's recordkeeping.

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

EVPD 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.

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."

Prior to the in-person portion of the audit, Chief Borscheid advised us that he could not locate documentation to verify that the public comment or public hearing requirements had been satisfied prior to the implementation of EVPD's BWC program. Rampart advised at that time to suspend the BWC program until an after-the-fact public hearing could be held. Chief Borscheid later provided documentation showing these requirements had been met. Specifically Chief Borscheid provided the following:

- Photographic documentation of a publicly-posted notice dated January 8th, 2025, notifying the public of a City Council meeting that would take place January 15th, 2025, and inviting comments from the public at the meeting as well as by submitting written letters or emails to the addresses in the notice.

[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 EVPD, these terms may be used interchangeably in this report.

- Copies of the minutes of the Eden Valley City Council Meeting dated January 15, 2025, which noted an agenda item number 2 opening a comment period to the public regarding body cameras. The minutes noted no one present to make comments and no written comments were received. A unanimous vote to approve body camera program was passed.

Copies of these documents have been retained in Rampart's audit files.

While Rampart recommends an after-the-fact public hearing as the only practical remedy when an agency is unable to verify that a public hearing was held prior to the implementation of its BWC program, because the legislature has not provided guidance on this subject, we are unable to express an opinion as to whether doing so satisfies the requirements of §626.8473 Subd. 2. We do note however that as of the date of our audit, EVPD had provided a public notice and held a public hearing regarding its BWC program.

Rampart verified that there was a working link to EVPD's BWC policy on the Police Department page of the City of Eden Valley website. In our opinion, EVPD is compliant with the requirements of §626.8473 Subd. 3(a).

EVPD BWC WRITTEN POLICY

As part of this audit, we reviewed EVPD'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 EVPD 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.

EVPD 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.

EVPD's BWC policy under Data Retention section A states that "[a]ll BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data." In our opinion, this satisfies the requirement of §13.825 Subd. 3(a).

EVPD's BWC policy under Data Retention states:

> 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, must be maintained for a minimum period of one year…Data documenting circumstances that have given rise to a formal complaint against an officer must be retained for six years.

The EVPD's BWC policy does not meet one of the requirements for categories of BWC data described in §13.825 Subd. 3(b). Specifically, it does not meet the one year minimum retention requirement for BWC data documenting any use of force by an officer that results in substantial bodily harm described in §13.825 Subd. 3(b).

Prior to the issuance of this report, EVPD submitted a revised BWC policy that adds the required one year retention period for BWC data documenting use of force that results in substantial bodily harm.

EVPD's BWC policy addresses the prohibition on altering, erasing or destroying BWC data and metadata prior to its scheduled expiration date, as described in Clause 2 of the Policy section of this report.

The policy addresses the 180 day additional retention requirement if requested in writing by a data subject.

EVPD currently possess a total of four (4) BWCS: Two (2) Axon-4 body-worn cameras are in regular use and two (2) older Vista wifi body-worn cameras are maintained as spares. EVPD used to use Watchguard Evidence Library on an in-house server, but it is no longer used and only kept for archived data from the Vista wifi era of use. If ever put out of service, EVPD is aware of its obligations of destruction under the FBI guidelines and will do so when the time is appropriate. EVPD currently utilizes Axon's Cloud storage and manages BWC data retention through automated retention settings in the 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 by the officers or supervisors. The preset classification is determined by officer assignment of call for service type (data classification) in the evidence.com software. If an officer fails to assign a data classification, the default retention period is indefinite until manually deleted or the classification is assigned.

Chief Borscheid advised that the Axon body-worn cameras utilize physical docking stations located at the EVPD, and that officers are responsible for docking their BWC for upload to the cloud at the end of their shift unless there is a critical incident (great bodily harm, death, officer involved shooting) in which case a supervisor or investigator would take over the BWC uploading duty.

In our opinion, EVPD's revised BWC policy is compliant with respect to applicable data retention requirements and a copy of the revised policy is attached to this report as Appendix B.

EVPD BWC Data Destruction

As discussed above, EVPD utilizes Axon's Evidence Library for storage, with retention periods determined based on the classification assigned to BWC data. Axon certifies that its Cloud Service is compliant with the Federal Bureau of Investigation'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.

FBI CJIS policy 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, EVPD's written BWC policy is compliant with respect to the applicable data destruction requirements.

EVPD BWC Data Access

Chief Borscheid advised us that that all requests for BWC data from the public or media are made in writing using a written request form available at the Police Department. This form is submitted to the Chief for processing and approval. An Axon evidence cloud link is sent to the requesting party to fulfill the data request. Requests from other law enforcement agencies or prosecutor's office or probation are submitted via email and follow the same process. We recommend stating the location for the public to access the data form or summarizing it within their BWC policy.

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. EVPD has language in their BWC policy to address these requirements.

Rampart notes that Section G of EVPD policy states:

> 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…BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

Chief Borscheid indicated that EVPD maintains verbal acknowledgments of any receiving agency's obligations under §13.825 Subd. 7 and Subd. 8, which include a requirement to maintain BWC data security. They also include a disclaimer in each email noting the receiving agency's obligations under statute. Rampart recommends obtaining written acknowledgements.

As discussed in Clauses 5 and 6 of the Policy section of this report, the Minnesota State Legislature provides 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 addressed these requirements using substantially similar language provided in statute.

Prior to the issuance of this report, EVPD submitted a data sharing form for LE and government agencies requiring a signature acknowledging their duties of security and destruction of BWC data and acknowledging the various provisions of MN Chapter 13 statutes. A copy of the sharing form has been retained in Rampart's audit file.

In our opinion, EVPD's written BWC policy is compliant with respect to the applicable

EVPD BWC Data Classification

EVPD's BWC Policy states that:

> 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.

The policy goes on to make distinctions between confidential and public data.

The policy implements the 2023 legislative changes regarding release of BWC data and the specific classifications when an individual dies as a result of a use of force by an officer. The language used is substantially similar to the text from statute.

In our opinion, this portion of policy is compliant with respect to the applicable data classification requirements.

EVPD BWC Internal Compliance Verification

The EVPD BWC Agency Use of Data section A states that "[s]upervisors will randomly review BWC usage to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required," a practice that Chief Borscheid confirmed he completes. All such reviews are logged in the evidence.com software. Chief Borscheid advised us that evidence.com software has an audit trail feature that logs all access.

The Use and Documentation section of EVPD's BWC policy states that "[o]fficers may use only department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this office."

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. EVPD's BWC policy uses identical language to address the statutory requirement.

EVPD's written BWC policy addresses consequences associated with violations of the policy, to include disciplinary action and criminal penalties.

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

EVPD BWC Program and Inventory

EVPD currently possesses four (4) BWC. There are two (2) actively used Axon Body-4 body-worn cameras and two (2) unused Vista wifi body-worn cameras.

The EVPD 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.

Chief Borscheid advised us that he is able to determine the number of BWCs deployed by reviewing the Axon GPS featured software and/or shift schedule.

As of the audit date, February 26, 2025, EVPD maintained 396.399GB of BWC data.

EVPD BWC Physical, Technological and Procedural Safeguards

EVPD BWC data are initially recorded to a hard drive in each officer's BWC. Data from each BWC is then uploaded to Axon's cloud service evidence.com via a physical docking station located at the Police Department. In the event an officer fails to label the video, the default retention period is indefinite until a label is assigned or it is manually deleted.

Only the Chief can delete BWC videos. Officers have view only powers of their BWC videos with the exception that they can edit labels for upload and retention. All BWC data access is logged automatically and available for audit purposes.

Enhanced Surveillance Technology

EVPD currently employs BWCs with only standard audio/video recording capabilities. EVPD 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.

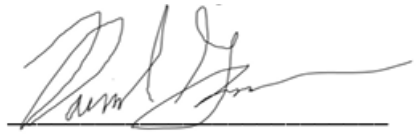
If EVPD should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses. EVPD specifically notes that this task should fall under the responsibility of the Police Department designated coordinator.

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 EVPD records.

Audit Conclusions

In our opinion, as of the date of our audit Eden Valley Police Department's Body-Worn Camera Program is substantially compliant with Minnesota Statutes §13.825 and §626.8473.



Rampart Audit LLC

5/06/2025

APPENDIX A:

Body-Worn Cameras

I. PURPOSE

The primary purpose of using body-worn-cameras (BWCs) is to capture evidence arising from police-citizen encounters. This policy sets forth guidelines governing the use of BWCs and administering the data that results. Compliance with these guidelines is mandatory, but it is recognized that officers must also attend to other primary duties and the safety of all concerned, sometimes in circumstances that are tense, uncertain, and rapidly evolving.

II. POLICY

It is the policy of this office to authorize and require the use of office-issued BWCs as set forth below, and to administer BWC data as provided by law.

III. PROCEDURE

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The chief or chief's designee may supersede this policy by providing specific instructions for BWC use to individual officers, or providing specific instructions pertaining to particular events or classes of events including, but not limited to, political rallies and demonstrations. The chief or designee may also provide specific instructions or standard operating procedures for BWC use to officers assigned to specialized details, for instance carrying out duties such as guarding prisoners or patients in hospitals and mental health facilities.

IV. DEFINITIONS

The following phrases have special meanings as used in this policy:

A. **MGDPA or Data Practices Act** refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq.

B. **Records Retention Schedule** refers to the General Records Retention Schedule for the Eden Valley Police Department.

C. **Law enforcement-related information** means information captured or available for capture by use of a BWC that has evidentiary value because it documents events with respect to a stop, arrest, search, citation, or charging decision.

D. **Evidentiary value** means that the information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or officer.

E. **General citizen contact** means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a wrecker, or receiving generalized concerns from a citizen about crime trends in

his/her neighborhood.

F. **Adversarial** means a law enforcement encounter with a person who becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward the other, or at least one person directs toward the other verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, or shouting. Encounters in which a citizen demands to be recorded or initiates recording on his/her own are deemed adversarial.

G. **Unintentionally recorded footage** is a video recording that results from an officer's inadvertence or neglect in operating the officer's BWC, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms, restrooms, and recordings made while officers were engaged in conversations of a non-business, personal nature, with the expectation that the conversation was not being recorded.

H. **Official duties,** for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this agency.

A. Use and Documentation

A. Officers may use only department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this office.

B. Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time, shall promptly report the malfunction to the on-duty supervisor and shall document the report. Supervisors and the reporting officer shall take prompt action to address malfunctions.

C. Officers should wear their issued BWCs 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.

D. Officers must document BWC use and non-use as follows:

1. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report or in the current Records Management System.

2. Whenever an officer fails to record an activity that is required to be recorded under this policy or captures only a part of the activity, the officer must document the circumstances and reasons for not recording in an incident report or the current Records Management System. Supervisors shall review these reports and initiate any corrective action deemed necessary.

E. The department will maintain the following records and documents relating to BWC use, which are classified as public data:

1. The total number of BWCs owned or maintained by the agency;

2. A daily record of the total number of BWCs actually deployed and used by officers;

3. The total amount of recorded BWC data collected and maintained; and

4. This policy, together with the Records Retention Schedule.

F. Officers assigned a BWC must 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.

B. Guidelines for Recording

A. Officers shall activate their BWCs when an officer activates their emergency overhead lights, responding to a call requiring an emergency response. Also, if an officer anticipates they will be involved in, become involved in, or witness other officers of this agency involved in a pursuit, *Terry* stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required, must be documented as specified in the Use and Documentation guidelines, part (D)(2) above.

B. Officers are not required to record general citizen contacts; however, they have the discretion to do so if deemed necessary.

C. Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded.

D. Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, officers should state the reasons for ceasing the recording on camera before deactivating their BWC and document in a written report. If circumstances change, officers shall reactivate their cameras, as required by this policy, to capture

information having evidentiary value.

E. Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy.

F. Notwithstanding any other provision in this policy, officers shall not use their BWCs to record other agency personnel during non-enforcement related activities, such as during pre- and post-shift time in locker rooms, during meal breaks, or during other private conversations, unless recording is authorized as part of an administrative or criminal investigation.

C. Guidelines for Recording Medical Issues

A. Officers need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value. When responding to an apparent mental health crisis or event, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.

B. Officers should consider using their BWCs and squad-based audio/video systems to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails, but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident.

D. Downloading

A. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his/her camera to designated location at the Eden Valley Police Department by the end of that officer's shift, with the discretion of the on-duty supervisor. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the officer's BWC and assume responsibility for transferring the data from it. Officers involved in those critical incidents shall not review the BWC video unless cleared to by the Chief of Police or his/her designee.

E. Administering Access to BWC Data

A. **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. The officer who collected the data.

3. 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.

B. **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:

1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.

2. Some BWC data is classified as confidential (see C. below).

3. Some BWC data is classified as public (see D. below).

C. **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.

D. **Public data.** The following BWC data is public:

1. 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.

2. Data that documents the use of force by a peace officer that results in substantial bodily harm.

3. 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 [*if practicable*]. In addition, any data on undercover officers must be redacted.

4. 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.

E. **Access to BWC data by non-employees.** Officers shall refer members of the media or public seeking access to BWC data to the Chief or Captain, who shall process the request in accordance with the MGDPA and other governing laws. In particular:

1. An individual shall be allowed to review recorded BWC data about himself/herself and other data subjects in the recording, but access shall not be granted:

a. If the data was collected or created as part of an active investigation.
b. 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:

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

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

c. 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.

F. **Access by peace officer and law enforcement employees.** No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes:

1. 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.

2. 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.

G. **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, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could 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,

1. 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.

2. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

3. 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;

4. 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, 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;

F. Data Security Safeguards

A. Password protected hard drive. The agency is unable to make backup copies of data.

B. Personally owned devices, including, but not limited to, computers and mobile devices, shall not be programmed or used to access or view agency BWC data.

C. Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the Chief. Apart from the following data as it cannot be erased:

- 1. Officers shall not erase or destroy any recording made with an 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.

D. As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this office shall obtain an independent biennial audit of its BWC program.

G. Agency Use of Data

A. Supervisors will randomly review BWC usage to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.

B. In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

C. Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.

D. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officers' objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field Training Officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainee's performance.

H. Data Retention

A. All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.

B. 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, must be maintained for a minimum period of one year.

C. Data documenting circumstances that have given rise to a formal complaint against an officer must be retained for six years.

D. Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.

E. Subject to Part F (below), all other BWC footage that is classified as nonevidentiary, becomes classified as non-evidentiary, or is not maintained for training, shall be destroyed after 90 days.

F. Upon written request by a BWC 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.

G. This office shall maintain an inventory of BWC recordings having evidentiary value.

I. Compliance

Supervisors shall monitor for compliance with this policy. The unauthorized access to or disclosure of BWC data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. § 13.09.

V. ACCOUNTABILITY

It is the responsibility of each employee to be familiar with and adhere to this directive. It is the responsibility of all supervisors to ensure this directive is followed. Failure to adhere to this directive may result in disciplinary action up to and including termination.

Reviewed 1/6/25

APPENDIX B:

Body-Worn Cameras

PURPOSE
The primary purpose of using body-worn-cameras (BWCs) is to capture evidence arising from police-citizen encounters. This policy sets forth guidelines governing the use of BWCs and administering the data that results. Compliance with these guidelines is mandatory, but it is recognized that officers must also attend to other primary duties and the safety of all concerned, sometimes in circumstances that are tense, uncertain, and rapidly evolving.

POLICY
It is the policy of this office to authorize and require the use of office-issued BWCs as set forth below, and to administer BWC data as provided by law.

PROCEDURE
This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The chief or chief's designee may supersede this policy by providing specific instructions for BWC use to individual officers, or providing specific instructions pertaining to particular events or classes of events including, but not limited to, political rallies and demonstrations. The chief or designee may also provide specific instructions or standard operating procedures for BWC use to officers assigned to specialized details, for instance carrying out duties such as guarding prisoners or patients in hospitals and mental health facilities.

DEFINITIONS
The following phrases have special meanings as used in this policy:

A. **MGDPA or Data Practices Act** refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq.

B. **Records Retention Schedule** refers to the General Records Retention Schedule for the Eden Valley Police Department.

C. **Law enforcement-related information** means information captured or available for capture by use of a BWC that has evidentiary value because it documents events with respect to a stop, arrest, search, citation, or charging decision.

D. **Evidentiary value** means that the information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or officer.

E. **General citizen contact** means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the

event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a wrecker, or receiving generalized concerns from a citizen about crime trends in his/her neighborhood.

F. **Adversarial** means a law enforcement encounter with a person who becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward the other, or at least one person directs toward the other verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, or shouting. Encounters in which a citizen demands to be recorded or initiates recording on his/her own are deemed adversarial.

G. **Unintentionally recorded footage** is a video recording that results from an officer's inadvertence or neglect in operating the officer's BWC, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms, restrooms, and recordings made while officers were engaged in conversations of a non-business, personal nature, with the expectation that the conversation was not being recorded.

H. **Official duties,** for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this agency.

Use and Documentation

A. Officers may use only department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this office.

B. Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time, shall promptly report the malfunction to the on-duty supervisor and shall document the report. Supervisors and the reporting officer shall take prompt action to address malfunctions.

C. Officers should wear their issued BWCs 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.

D. Officers must document BWC use and non-use as follows:

1. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report or in the current Records Management System.

2. Whenever an officer fails to record an activity that is required to be recorded under this policy or captures only a part of the activity, the officer must document

the circumstances and reasons for not recording in an incident report or the current Records Management System. Supervisors shall review these reports and initiate any corrective action deemed necessary.

E. The department will maintain the following records and documents relating to BWC use, which are classified as public data:

1. The total number of BWCs owned or maintained by the agency;

2. A daily record of the total number of BWCs actually deployed and used by officers;

3. The total amount of recorded BWC data collected and maintained; and

4. This policy, together with the Records Retention Schedule.

F. Officers assigned a BWC must 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.

Guidelines for Recording

A. Officers shall activate their BWCs when an officer activates their emergency overhead lights, responding to a call requiring an emergency response. Also, if an officer anticipates they will be involved in, become involved in, or witness other officers of this agency involved in a pursuit, *Terry* stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required, must be documented as specified in the Use and Documentation guidelines, part (D)(2) above.

B. Officers are not required to record general citizen contacts; however, they have the discretion to do so if deemed necessary.

C. Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded.

D. Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing,

officers should state the reasons for ceasing the recording on camera before deactivating their BWC and document in a written report. If circumstances change, officers shall reactivate their cameras, as required by this policy, to capture information having evidentiary value.

E. Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy.

F. Notwithstanding any other provision in this policy, officers shall not use their BWCs to record other agency personnel during non-enforcement related activities, such as during pre- and post-shift time in locker rooms, during meal breaks, or during other private conversations, unless recording is authorized as part of an administrative or criminal investigation.

Guidelines for Recording Medical Issues

A. Officers need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value. When responding to an apparent mental health crisis or event, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.

B. Officers should consider using their BWCs and squad-based audio/video systems to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails, but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident.

Downloading

A. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his/her camera to designated location at the Eden Valley Police Department by the end of that officer's shift, with the discretion of the on-duty supervisor. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the officer's BWC and assume responsibility for transferring the data from it. Officers involved in those critical incidents shall not review the BWC video unless cleared to by the Chief of Police or his/her designee.

Administering Access to BWC Data

A. **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. The officer who collected the data.

3. 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.

B. **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:

1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.

2. Some BWC data is classified as confidential (see C. below).

3. Some BWC data is classified as public (see D. below).

C. **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.

D. **Public data.** The following BWC data is public:

1. 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.

2. Data that documents the use of force by a peace officer that results in substantial bodily harm.

3. 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 [*if practicable*]. In addition, any data on undercover officers must be redacted.

4. 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.

E. **Access to BWC data by non-employees.** Officers shall refer members of the media or public seeking access to BWC data to the Chief, who shall

process the request in accordance with the MGDPA and other governing laws. In particular:

1. An individual shall be allowed to review recorded BWC data about himself/herself and other data subjects in the recording, but access shall not be granted:

a. If the data was collected or created as part of an active investigation.
b. 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:

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

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

c. 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.

F. **Access by peace officer and law enforcement employees.** No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes:

1. 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.

2. 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.

G. **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, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could 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,

1. 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.

2. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

3. 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;

4. 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, 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;

Data Security Safeguards

A. Password protected hard drive. The agency is unable to make backup copies of data.

B. Personally owned devices, including, but not limited to, computers and mobile devices, shall not be programmed or used to access or view agency BWC data.

C. Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the Chief. Apart from the following data as it cannot be erased:

- 1. Officers shall not erase or destroy any recording made with an 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.

D. As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this office shall obtain an independent biennial audit of its BWC program.

Agency Use of Data

A. Supervisors will randomly review BWC usage to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.

B. In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

C. Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.

D. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officers' objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field Training Officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainee's performance.

Data Retention

A. All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.

B. 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, must be maintained for a minimum period of one year.

C. Data documenting circumstances that have given rise to a formal complaint against an officer must be retained for six years.

D. Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.

E. Subject to Part F (below), all other BWC footage that is classified as nonevidentiary, becomes classified as non-evidentiary, or is not maintained for training, shall be destroyed after 90 days.

F. Upon written request by a BWC 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.

G. This office shall maintain an inventory of BWC recordings having evidentiary value.

H. Any BWC recording of an officer's use of force resulting in substantial bodily harm shall be retained for at least one year.

I. The following are the BWC categories and how long the data is retained:

Uncategorized	Until manually deleted
A Warning	90 days
Alarm	180 days
Animal	180 days
Arrest	3 years
Assault	3 years
Burglary/Theft	Until manually deleted
Citation Issued	2 years
Civil	180 days
Crash - Injury/Fatal	Until manually deleted
Crash - No Injuries	180 days
Death Investigation	Until manually deleted

Domestic	Until manually deleted
DWI	Until manually deleted
Juvenile Trouble	180 days
Medical	180 days
Mental Health	180 days
Miscellaneous	Until manually deleted
Pursuit	Until manually deleted
Search Warrant	3 years
Statement	Until manually deleted

Compliance
Supervisors shall monitor for compliance with this policy. The unauthorized access to or disclosure of BWC data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. § 13.09.

ACCOUNTABILITY
It is the responsibility of each employee to be familiar with and adhere to this directive. It is the responsibility of all supervisors to ensure this directive is followed. Failure to adhere to this directive may result in disciplinary action up to and including termination.

Revised 3/3/25