INDEPENDENT AUDITOR'S REPORT

St. Cloud Police Department Body-Worn Camera Program

MARCH 13, 2023

RAMPART DEFENSE LLC
P.O. Box 23 Clearbrook, MN 56634

Audit Overview and Recommendations

Dear St. Cloud City Council and Chief Oxton:

We have audited the body-worn camera (BWC) program of the St. Cloud Police Department (SCPD) for the period of 2/28/2021 - 1/30/2023. 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 St. Cloud Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On February 24, 2023, Rampart Defense LLC (Rampart) met with Lieutenant Jason Burke, who provided information about SCPD'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 SCPD's recordkeeping.

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

SCPD 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.

Lt. Burke provided links to the following documents as evidence that SCPD had met these requirements:

1. The December 7, 2021, St. Cloud City Council Meeting Minutes, which note the scheduling of a public hearing on December 21, 2021, "TO ALLOW FOR PUBLIC COMMENT AND TO AUTHORIZE THE MAYOR AND CITY CLERK TO ENTER INTO A CONTRACT TO PURCHASE THE BODY WORN CAMERA SYSTEM."
2. A media release dated December 8, 2021, announcing the proposed body-worn camera program and inviting the public to submit written comments via mail or email, or to provide in-person comments at the December 21, 2021, public hearing.

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

3. The December 21, 2021, St. Cloud City Council Meeting Minutes, which note that a public hearing was opened to receive comments regarding the proposed BWC system. After the public hearing was closed, the city council voted to approve a resolution to authorize the mayor and city clerk to proceed with the proposed purchase.
4. A certified copy of the resolution authorizing purchase of a body-worn camera system.

Copies of these documents have been retained in Rampart's audit files. In our opinion, St. Cloud Police Department met the public notice and comment requirements prior to the implementation of their BWC program.

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

Lt. Burke furnished to Rampart a copy of SCPD's written BWC policy, as well as a link to SCPD's BWC policy, which was posted on the City of St. Cloud's website. Rampart verified that this link worked at the time of receipt. We noted that SCPD maintains a webpage dedicated to providing information about their BWC program, including links to the governing statutes, records retention schedule and the form used to request BWC footage. In our opinion, St. Cloud Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

SCPD BWC WRITTEN POLICY

As part of this audit, we reviewed SCPD'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. Procedures for testing the portable recording system to ensure adequate functioning;
3. Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
4. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
5. Circumstances under which a data subject must be given notice of a recording;
6. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
7. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
8. Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

Due to their complexity and interrelatedness, clauses 1 and 7 are discussed separately below. Clause 8 is also discussed separately.

In our opinion, the SCPD BWC policy is compliant with respect to clauses 2 – 6.

SCPD BWC Data Retention

St. Cloud Police Department follows the General Records Retention Schedule for Minnesota Cities (GRRSMC) with respect to BWC data classified as having evidentiary value. SCPD's BWC policy defines this to include "information [that] 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." A review of the relevant sections of the current GRRSMC schedule indicates that the stated retention guidelines appear to meet or exceed the requirements specified for each category of BWC data enumerated in §13.825 Subd. 3(b). These categories are also addressed specifically in the written policy, and include the required retention periods. SCPD's policy specifies 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," as required in §13.825 Subd. 3(a). Finally, SCPD's policy notes that "[w]hen a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period."

SCPD employs Axon Body 3 (AB3) body-worn cameras and utilizes Axon's Cloud Service storage (Evidence.com). SCPD manages BWC data retention through automated retention settings in Axon's video management software. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be adjusted as needed.

SCPD's BWC policy states that "[e]ach officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to the secure storage system by the end of that officer's shift." This is accomplished by physically docking BWCs at the St. Cloud Police Department in order to upload the data. Officers are required to assign the appropriate data label or labels to each file at the time of capture or transfer to storage.

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

SCPD BWC Data Destruction

As discussed above, SCPD utilizes Axon's Evidence.com 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 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.

BWC data determined to be evidentiary in nature are marked "manual deletion only" to avoid the accidental loss of data. Lt. Burke identified five (5) employees who are authorized to delete BWC videos manually, and advised that this is done only upon receipt of a case outcome report from the prosecutor's office documenting that the case is complete. BWC data marked for deletion enter a queue where they remain for approximately 10 days as a further safeguard against accidental deletion.

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

SCPD BWC Data Access

SCPD's BWC policy states that officers shall refer "members of the media or public seeking access to BWC data to the department's BWC Video Request Form and Instructions." A review of that form shows that the requester is directed to submit the completed form to the SCPD front desk. All such requests are processed by Records staff "in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws." BWC videos are shared with members of the public via an emailed internet link.

SCPD's BWC policy also 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." In addition, BWC data "shall be made available to prosecutors, courts, and other criminal justice entities as provided by law."

Requests for BWC data from outside law enforcement agencies are primarily directed to Records staff; however, because Evidence.com is unable to separate photo sharing rights from video sharing rights, SCPD officers are authorized to share both with partner agencies. All shared files are logged in Evidence.com, to include the requester and the form of the request, and this sharing is subject to audit. All such requests are fulfilled via Axon's partner sharing function, if the requesting agency is also an Axon client, or else via a downloadable internet link.

As of the date of the audit, the St. Cloud City Attorney's Office and the Benton, Sherburne and Stearns County Attorney's Offices all receive BWC video via Axon's partner sharing function. Prosecutor requests utilize a specific digital evidence request form.

Lt. Burke advised us that while there is a verbal understanding among partner agencies of their obligations under §13.825 Subd. 7 and Subd. 8, including a requirement to maintain BWC data security, SCPD is also exploring options to add a disclosure statement or otherwise obtain written acknowledgement of these obligations.

We recommend that SCPD obtain written acknowledgement from partner agencies of their §13.825 Subd. 7 and Subd. 8 responsibilities. This can be accomplished through a disclosure statement, a mandatory check box on the data request form or via a separate email from each agency requesting BWC data. These acknowledgements should be maintained on file.

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

SCPD BWC Data Classification

SCPD's BWC Policy states that "BWC data is presumptively private," and 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. SCPD BWC Policy also identifies certain categories of BWC data that are public.

This section of the SCPD BWC policy mirrors the categories and language of §13.825 Subd. 2. In our opinion, this policy is compliant with respect to the applicable data classification requirements.

SCPD BWC Internal Compliance Verification

The SCPD BWC Policy Agency Use of Data section states that "[s]upervisors shall monitor for compliance with this policy," and also states that:

> At least once a quarter, supervisors will randomly review BWC usage by each officer to whom a BWC is issued or available for use, to ensure compliance with this policy.
>
> 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.

Lt. Burke advised us that as of the beginning of 2023, the policy has been revised to require monthly rather than quarterly checks, with a minimum of two (2) videos reviewed per officer. All reviews are logged and subject to audit by SCPD administration.

Though not required by statute, we recommend that the monthly supervisory reviews include a sampling of the recordings created by the start-of-shift function testing mandated in SCPD's BWC policy.

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

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

SCPD BWC Program and Inventory

SCPD currently possesses 122 Axon Body 3 body-worn cameras.

The SCPD 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. Officers' body-worn cameras are synced to both their squad's emergency lights and their Tasers, and are automatically activated anytime those devices are activated.

Lt. Burke advised us that he is able to determine the number of BWCs deployed by reviewing the schedule and/or payroll data.

As of January 8, 2023, SCPD maintained 88,391 BWC data files, of which 87,123 were active. The remaining videos were queued for deletion.

SCPD BWC Physical, Technological and Procedural Safeguards

SCPD BWC data are initially recorded to a hard drive in each officer's BWC. Prior to the end of each shift, the officer places his or her BWC in a docking station at SCPD. Any BWC data are then uploaded automatically to Evidence.com. BWC administrators review and classify any unlabeled videos to avoid the accidental loss of data.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes. Officers are required to document the reasons for accessing BWC data each time they do so. All BWC data access is logged automatically and available for audit purposes.

Enhanced Surveillance Technology

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

If SCPD 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 ICRs 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 this audit covers a period of twenty-three months, while most BWC data is only required to be retained for 90 days, there is a significant likelihood that the sample population will include ICRs for which BWC data was created, but which has since been deleted due to the expiration of the retention period. The auditors reviewed the retained BWC videos to determine whether this data was accurately documented in SCPD records.

We noted numerous instances of videos labeled with the incorrect ICR number during our review, and observed that this occurred across several different officers, while also observing instances in which individual officers mislabeled multiple videos. Upon further investigation, we determined that one (1)

video was labeled with the CFS (call for service) number rather than the ICR number. We also noted instances in which multiple ICR numbers were accidentally created for a single call. When this happens, one of the ICR numbers is marked inactive, while the other remains active. In these instances, some or all of the related videos were labeled with the inactive ICR number rather than the active ICR number. Finally, we noted that the majority of the remaining instances involved labeling BWC videos with ICR numbers of other calls to which that officer had responded during that same shift.

From our review of these videos, it appears that the mislabeling we observed is the result of inattentiveness by officers, who consistently categorized the videos correctly for retention purposes. We noted a high BWC utilization rate on calls, with video having been created on 94 of 132 reviewed ICRs (71%). We also noted that a total of 215 BWC videos were linked to these 94 ICRs. Given St. Cloud Police Department's large call volume and high BWC utilization rate, it is likely that each officer is labeling numerous BWC videos at the end of each shift, a process that requires selecting the video, locating the associated ICR number in the RMS and either manually entering or copying-and-pasting that ICR number into Evidence.com. Such a process could easily result in errant labeling, particularly if an officer is rushing to mark multiple videos at the end of his or her shift.

After discussing our concerns with Lt. Burke, he was able to identify a manual search process SCPD can employ to ensure that BWC data are correctly identified, particularly when responding to requests from data subjects. While this process is somewhat time-consuming, it does appear to be effective in ensuring that requested BWC data are correctly identified.

We strongly recommend that SCPD conduct an internal audit or other review of its BWC video labeling procedures to identify underlying causes of mislabeling and determine steps to mitigate this issue.

Audit Conclusions

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

Daniel E. Gazelka

Rampart Defense LLC

3/13/2023

Appendix A:

ST CLOUD POLICE DEPARTMENT

Law Enforcement

Policies and Procedures

Subject: Body Worn Cameras (BWC)	Policy Number: 235
Issue Date: 02-02-2021	Revision Date:
Approval Authority - Title and Signature: Wm. Blair Anderson, Chief of Police	

POLICY

It is the policy of this department to authorize and require the use of department-issued body-worn-cameras (BWCs) as set forth below, and to administer BWC data as provided by law.

PURPOSE

The use of BWCs by the Saint Cloud Police Department is intended to enhance the mission of the Department by documenting contacts between members of the Department and the public, while balancing demands of accountability, transparency, and privacy concerns. 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.

AUTHORITY

Minnesota Statute 626.8473 and 13.825

SCOPE

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of surreptitious recording devices in undercover operations or the use of squad-based (dash-cam) video recorders. The Chief of Police and/or their designee may modify this policy by providing specific instructions for the use of BWCs to individual officers or providing specific instructions for the use of BWCs pertaining to certain events or classes of events. The Chief of Police and/or their designee may also provide specific instructions or standard operating procedures for BWC use to officers assigned to specialized details, such as guarding prisoners or patients in hospitals and mental health facilities.

DEFINITIONS

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

A. **Body Worn Camera** refers to a portable recording device worn by a peace officer that is capable of both video and audio recording of the officer's activities and interactions with others or collecting digital multimedia evidence as part of an investigation.

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

C. **Records Retention Schedule** refers to the General Records Retention Schedule for Minnesota Cities.

D. **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.

E. **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.

F. **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 tow truck, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.

G. **Adversarial contact** means a law enforcement encounter with a person that 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 or her own are deemed adversarial.

H. **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.

I. **Critical incident** refers to an encounter between a police officer and community member(s) that results in great bodily harm or death to a community member or the officer. A critical incident could include an officer use of force or deadly force encounter between a police officer and a member of the community. A critical incident may also include an in-custody death of a person under the care, custody, or control of an officer.

J. **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.

PROCEDURE

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 department.

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 officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing.

c. Officers shall wear their issued BWCs at the location on their body and in the manner specified in training.

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 Computer-Aided Dispatch (CAD) record of the event.

2. Whenever an officer fails to record an activity that is required to be recorded under this policy or fails to record for the entire duration of the activity, the officer must document the circumstances and reasons for not recording in an incident report or CAD record of the event and report the incident to their supervisor. Supervisors shall review these incidents 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.

B. General Guidelines for Recording

a. Officers shall activate their BWCs when responding to all calls for service, prior to interacting with those involved in the respective incident, and during all law enforcement-related encounters and activities, including, but not limited to, traffic stops, pursuits, investigative stops of motorists and pedestrians, arrests, searches, uniformed officers' interviews and interrogations of suspects, and during any police/citizen contacts that become adversarial. 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 thoroughly documented as specified in the Use and Documentation guidelines, part (D)(2) (above).

b. Except as otherwise directed, officers have discretion to record or not record general citizen contacts.

c. Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded. Officers may elect to notify people they encounter that a BWC is being operated if it is felt that doing so may aid the law enforcement process, reduce fear on the part of a person subjected to a law enforcement contact, result in improved behavior of a person, or if it serves to de-escalate an encounter. If asked, officers are required to provide a factual response about recording.

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. In an incident where a sergeant is in charge of the scene, he/she shall direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. 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. All officers participating in the service of a search warrant shall wear and record the execution of the search warrant. Based on the circumstances, the on-scene sergeant may direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value.

g. Department personnel assigned to a plain clothes, investigative assignment, undercover assignment, or uniformed/plain clothes administrative role shall not be required to wear a

BWC during their day-to-day work unless working in a uniformed call response capacity or are otherwise required by this policy (covered in Section B (a.)) or a command-level directive.

h. 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. Special Guidelines for Recording

Officers may, in the exercise of sound discretion, determine:

a. To use their BWCs to record any police-citizen encounter if there is reason to believe the recording would potentially yield information having evidentiary value, unless such recording is otherwise expressly prohibited.

b. Officers shall use their BWCs and, if so equipped, 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 and Labeling Data

a. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to the designated data storage location by the end of that officer's shift. 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 shall take custody of the officer's BWC and assume responsibility for transferring the data from it. If the incident is being investigated by an outside authority, the involved officer's BWC shall be turned over to the investigating authority before the data is transferred from the camera device.

b. Officers shall label the BWC data files at the time of capture or transfer to storage and should consult with a supervisor if in doubt as to the appropriate labeling. Officers should assign as many of the following labels as are applicable to each file:

Classification	**Definition**	**Retention**
Test/Accidental	Test/Accidental Activation/Non-Evidence	90 Days
Call for Service	Call for Service/General Citizen Contact	180 Days
Traffic Stop/Crash	Traffic Stops/Crashes	180 Days
Adversarial Contact	Incident Involving Adversarial Contact	180 Days
Discharge of Firearm	By a Peace Officer in the Course of Duty, other than for Training Purposes or the	1 Year

	Killing of an Animal that is Sick, Injured, or Dangerous	
Use of Force/Fleeing	Use of Force/Fleeing	7 Years
Evidence	Arrest/Referral of Charges/Evidence	7 Years*
Internal Investigations	Internal Investigation	5 Years**
Formal Complaint	Formal Complaint Made Against Peace Officer	1 Year
Death/CSC	Death/Criminal Sexual Conduct Investigation	Permanent

* Data will be retained for 7 years or until manually deleted after final case disposition
** Data will be retained for 5 years after separation/termination

c. In the event of unintentional BWC recording that captures sensitive personal information that should be restricted, an officer may submit a written request via email to the Commander of Support to restrict access to that portion of BWC data. The Commander will evaluate the request with the Chief of Police and/or their designee. If a restriction is placed on access to such data, that restriction will remain until the data is deleted according to the retention schedule of the data's category.

d. Labeling designations may be corrected or amended based on additional information.

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** is 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. With the approval of the Chief of Police and/or their designee, this department may make otherwise non-public data public data if that could aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest, consistent with Minnesota Statutes, section 13.82, subdivision 15.

f. **Access to BWC data by non-employees**. Officers shall refer members of the media or public seeking access to BWC data to the department's BWC Video Request Form and Instructions. Once received, the request will be processed in accordance with the MGDPA and other governing laws. In particular:

1. 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:

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.

g. **Access by peace officers 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. Officers may access and view stored BWC video, including their own, only when there is a clear and legitimate business need for doing so, including but not limited to:
        a. To prepare a police report, draft a search warrant, prepare for an interview, or locate potential evidence stemming from a call for service or officer-initiated police activity.

        b. To prepare for court testimony.

        c. When authorization has been given under subdivisions 2 and 3 of this section.

    2. Officers are prohibited from reviewing related BWC footage, including their own, following a police-citizen critical incident that results in great bodily harm or death to a citizen.

        a. After consultation with the officer, the officer's legal representation, and the agency conducting the investigation, the Chief of Police and/or their designee may authorize the officer to review their BWC footage prior to filing a report or giving a statement.

    3. Upon notification of being a witness or subject of an internal investigation, officers are prohibited from reviewing related BWC footage, including their own, unless authorization is given by the Chief of Police and/or their designee.

    4. Agency personnel shall document their reasons for accessing stored BWC data in the Evidence.com system 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.

5. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Approval to utilize video footage for law enforcement training purposes must be approved by the Chief of Police and/or their designee. BWC footage used for law enforcement training purposes shall be redacted prior to use. Field training officers may review BWC data with trainees for the purpose of providing coaching and feedback on the trainee's performance.

6. 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.

h. **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 individual identities that are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screenshots, 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.

F. Data Security Safeguards

a. BWC data will be securely stored by utilizing Evidence.com by Axon.

b. Personal-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 of Police and/or their designee.

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

G. Agency Use of Data

a. At least once a quarter, supervisors will randomly review BWC usage by each officer to whom a BWC is issued or available for use, to ensure compliance with this policy.

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. 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.

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 1 year.

c. Certain kinds of BWC data must be retained for seven years:

    1. Data that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report or supervisory review.

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

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 non-evidentiary, 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. The department shall maintain an inventory of BWC recordings having evidentiary value by utilizing the Evidence.com database by Axon.

The department will post this policy, together with its Records Retention Schedule, on its website.