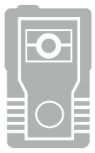
INDEPENDENT AUDITOR'S REPORT

St. Cloud Police Department



APRIL 4TH, 2025

RAMPART AUDIT LLC

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 two-year period of 1/31/2023 - 1/30/2025. 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 St. Cloud Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On February 21, 2025, Rampart Audit LLC (Rampart) met with Lieutenant Jason Burke and Lieutenant Justin Day, 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.

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

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

[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.

1. The December 7, 2020, St. Cloud City Council Meeting Minutes, which note the scheduling of a public hearing on December 21, 2020, "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, 2020, 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, 2020, public hearing.
3. The December 21, 2020, 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.

Rampart staff verified that the BWC policy was accessible from the St. Cloud Police Department's webpage at the time of our audit. 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 met the public notice and comment requirements prior to the implementation of their BWC program.

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. A prohibition on altering, erasing or destroying any recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely;
3. A mandate that a portable recording system be worn at or above the mid-line of the waist in a position that maximizes the recording system's capacity to record video footage of the officer's activities;
4. A mandate that officers assigned a portable recording system wear and operate the system in compliance with the agency's policy adopted under this section while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official;

5. A mandate that, notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the deceased individual's next of kin, the legal representative of the deceased individual's next of kin, and the other parent of the deceased individual's child, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, with the following exception:
    - A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to section 13.82 subdivision 7;
6. A mandate that, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82 subdivision 7;
7. Procedures for testing the portable recording system to ensure adequate functioning;
8. Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
9. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
10. Circumstances under which a data subject must be given notice of a recording;
11. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
12. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
13. Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

In our opinion, the SCPD 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.

SCPD 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.

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 most recent GRRSMC schedule Rampart was able to locate online, dated 2021, 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(a), (b) and (d), but do not address the "indefinite" retention requirement for data described in §13.825 Subd. 3(c), which was updated by the Minnesota State Legislature in 2023.

In addition to the retention guidelines contained in the GRRSMC, these categories are also addressed specifically in the Data Retention section of SCPD's BWC policy. Subsection (a) of the Data Retention section of 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). Subsection (c) of the Data Retention section of SCPD's policy prescribes a retention period of one year for BWC data documenting a reportable firearms discharge, while subsection (d) establishes a retention period of seven years for BWC data documenting "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," which appear to meet or exceed the requirements of §13.825 Subd. 3(b). Subsection (b) of the Data Retention section of SCPD's BWC policy addresses the requirements of §13.825 Subd. 3(c) thusly: "All BWC data documenting a peace officer using deadly force must be maintained indefinitely." Subsection (g) of the Data Retention section of SCPD's BWC policy addresses the additional retention requirement discussed in §13.825 Subd. 3(d).

While we noted that the retention period for data documenting an officer's use of deadly force is listed as seven years in subsection (d) and indefinite in subsection (b), SCPD's policy also notes that "[w]hen a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period." We recommend that SCPD remove the reference to "the use of deadly force by a peace officer" under subsection (d) to improve clarity.

SCPD staff advised us that if an officer fails to assign a category to a BWC recording, the retention setting "until manually deleted" is assigned to avoid the accidental loss of data. Unclassified recordings are periodically reviewed and assigned the proper category, which then resets the retention period accordingly.

Subsection (c) of the Data Security Safeguards section of SCPD's BWC policy states: "Officers shall not intentionally edit, alter, or erase any BWC recording unless expressly authorized by the Chief of Police and/or their designee."

As discussed in Clause 2 of the Policy section of this report, a BWC policy must prohibit altering, erasing or destroying any recording made with a peace officer's portable recording system, as well as associated data or metadata, prior to the expiration of the applicable retention period. In addition, the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely. At the time of our audit, SCPD's BWC policy did not address these requirements.

Prior to the submission of this report, SCPD furnished an updated BWC policy that addresses the concerns related to retention noted in this section. A copy of this revised policy has been attached to this report as Appendix B.

AUDITOR'S NOTE: St. Cloud Police Department personnel voiced concerns about the following portion of Minn. Stat. §626.8473 Subd. 3(b)(1): "…The policy must prohibit altering, erasing, or destroying any recording made with an officer's portable recording system or data and metadata related to the recording prior to the expiration of the applicable retention period under section 13.825, subdivision 3…" "Related data and metadata" is commonly understood to refer to information such as labels and tags that are used to link a recording to a particular call or incident, and to categorize the recording to determine its retention period within a video management system. While it is Rampart's opinion that the legislative intent behind this language was to prohibit changes made for nefarious purposes, such as assigning an incorrect call number to make a recording difficult to locate or assigning an incorrect classification to cause a recording's retention to expire prematurely, a strict reading of the statutory language does appear to prohibit any modifications whatsoever, including not only necessary acts, such as correcting inadvertent labelling or categorization errors, but also mandatory acts, such as extending a recording's retention period when so requested by a data subject under §13.825 Subd. 3(d). For that reason, SCPD has added language to their policy clarifying that the prohibition against editing, altering, or erasing data or metadata "does not include an officer's ability to correct errant BWC metadata." In our opinion, this modification is an appropriate means of addressing a deficiency in the statutory language.

SCPD employs Axon Body 3 (AB3) and Body 4 (AB4) 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 designated data storage location 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. During our previous audit, SCPD personnel 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 reviewed by a lieutenant and 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 DVD or 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.

SCPD advised Rampart that all requests fulfilled for other law enforcement agencies are accompanied by a written notice reminding the receiving agency of their obligations under §13.825 Subd. 8 (c), §13.05 Subd. (5) and §13055, including a requirement to maintain BWC data security. SCPD furnished a copy of this notice as part of this audit. Rampart has retained a copy in our audit files.

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.

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. Subsection (f) of the Administering Access to BWC Data section of SCPD's BWC policy addresses the access requirements pertaining to survivors and legal counsel, while subsection (g) addresses the public release requirements for BWC data that document an officer's use of deadly force. Both subsections quote extensively from the governing statutory language.

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. As noted in the preceding section, SCPD has also revised its BWC policy to reflect the 2023 legislative updates.

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

Subsection (e) of the Agency Use of Data section of the SCPD BWC policy states that: "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."

Subsection (b) of the Agency Use of Data section of the SCPD BWC policy states that:

> Every month, 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. This review will include a minimum of two BWC videos created by each officer…

All reviews are logged and subject to audit by SCPD administration.

Subsection (c) of the Use and Documentation section of the SCPD BWC policy states that: "Officers assigned a BWC shall wear and operate the system in compliance with this agency's policy while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official." In our opinion, this satisfies the requirements discussed in Clause 4 of the Policy section of this report.

In our opinion, SCPD's BWC 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 a total of 132 Axon body-worn cameras, which consist of a mix of AB3 and AB4 models. Of those 132 BWCs, 119 are assigned and in regular use while the remaining 13 are held as spares.

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.

While SCPD does not maintain a separate log of BWC deployment or use, because each patrol officer wears a BWC while on duty, deployment can be determined based on a review of schedule and payroll records. Actual BWC use would be determined based on the creation of BWC data.

As of February 21, 2025, SCPD maintained 147,323 BWC data files, totaling 91,322.6 GB.

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.

As discussed in Clause 3 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must specify that a BWC be worn at or above the mid-line of the waist. Subsection (d) of the Use and Documentation section of SCPD's BWC policy states:

> Officers in uniform, to include officers wearing any type of outer tactical vest carrier, who are required to wear a BWC, shall 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 footage of the officer's activities. The mid-line of the waist will be one inch above the officer's navel.

Because §626.8473 Subd. 3(b)(2) does not limit the requirement that a BWC be worn at or above the mid-line of the waist only to uniformed personnel, we recommend that SCPD amend their BWC policy to direct all personnel using a BWC to wear it at or above the mid-line of the waist. Prior to the completion of this report, SCPD submitted a revised BWC policy that addresses this.

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 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 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.

Rampart previously audited St. Cloud Police Department's BWC program in 2023. At that time, we noted a high incidence of mislabeled BWC recordings and recommended that SCPD review its BWC labeling procedures to identify underlying causes, as well as to determine steps to mitigate the issue.

During our current audit, we noted that the labeling error rate showed significant improvement from our previous audit. While we recommend that SCPD continue their efforts to further reduce the labeling error rate, the progress we observed was noteworthy.

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.

Rampart Audit LLC

4/04/2025

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: 05-21-24; 06-04-24; 11-22-24; 12-09-24
Approval Authority - Title and Signature: Jeffrey Oxton, 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

Minn. Stat. §626.8473 and Minn. Stat. §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 (BWC)** 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. **UMD** refers to Until Manually Deleted relating to the storage of BWC recordings in Axon Evidence.

E. **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.

F. **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.

G. **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.

H. **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.

I. **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, BWC function test, recordings made in station house locker rooms, and 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.

J. **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's 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.

K. **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. A function test shall consist of the operator undocking the BWC, activating then stopping a recording to confirm the device is working 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 assigned a BWC shall wear and operate the system in compliance with this agency's policy while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official.

d. Officers in uniform, to include officers wearing any type of outer tactical vest carrier, who are required to wear a BWC, shall 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 footage of the officer's activities. The mid-line of the waist will be one inch above the officer's navel.

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

1. Whenever an officer makes a recording relating to a CFS, the existence of the recording shall be documented in an incident report or Computer-Aided Dispatch (CAD) record of the event. An exception to this requirement would be recordings that are test/accidental/non-evidentiary citizen contacts in nature.

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.

f. 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 while responding to all calls for service prior to arriving on scene and interacting with those involved in the respective incident (whether in person or via phone), 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 in the General Guidelines for Recording, part a (above), officers have the discretion to record or not record general citizen contacts, contracted overtime activities, and extra or directed patrols.

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. Livestreaming BWC video utilizing WatchMe

a. WatchMe is a livestreaming feature that allows the end operators to initiate a request for an authorized user to livestream the operator's actively recording BWC video and audio.

1. Authorized users that receive the request and have the ability to livestream BWC video and audio will be Sergeants, Lieutenants, Commanders, Assistant Chief of Police, and the Chief of Police.

2. This policy does not mandate the use of the WatchMe feature by the end operator, nor does it mandate an authorized user to accept the request and livestream the BWC video and audio.

3. In limited circumstances, a supervisor can direct an officer to activate the WatchMe feature while on an active call for service which may necessitate supervisor response or guidance and physical response cannot readily be achieved. This does not replace the need for a supervisor to respond to the scene when able to do so. This type of directive will require the supervisor to notify their chain of command via email and provide a brief explanation of the situation, and the need for the directive.

E. 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 to Axon Evidence.

b. Officers shall accurately label the BWC data files at the time of capture, or prior to the 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 category labels as are applicable to each file:

Category Label	**Definition**	**Retention**	**Category Duration**
1-Test/Accidental/CC	Test/Accidental Activation/Non-Evidentiary Citizen Contact	See Category Duration	90 Days
No Report	Call for Service cleared in CAD/Traffic Stop/Crash No Citation/General Citizen Contact/Adversarial Contact/Transport	See Category Duration	1 Year
Report-RMS	RMS Report completed/Citation Issued/ Arrest Made	See Record Retention Schedule*	UMD
Discharge of Firearm	By a Peace Officer in the Course of Duty, other than for Training Purposes or the Killing of an Animal that is Sick, Injured, or Dangerous	1 Year	1 Year
Use of Force/Fleeing	Use of Force/Fleeing	See Record Retention Schedule	7 Years
Internal Investigations	Internal Investigation	See Record Retention Schedule **	UMD

Formal Complaint	Formal Complaint Made Against Peace Officer	See Record Retention Schedule	1 Year
Death/CSC	Death/Criminal Sexual Conduct Investigation	See Record Retention Schedule	UMD
Specialty/Restricted	VOTF/CMHTTF/SWAT	See Record Retention Schedule	7 Years

* Data will be manually deleted after final case disposition, or statute of limitations has expired
** 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.

F. 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 Minn. Stat. §13.82, subd. 15.

f. **Death resulting from force—access to data by survivors and legal counsel.** Notwithstanding any other law or policy to the contrary, when an individual dies as a result of force used by an officer of this agency, all BWC data documenting the incident, redacted only as required by law, must be made available for inspection by any of the following individuals within five days of their request:

1. The deceased individual's next of kin;

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

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

The request may be denied if there is a compelling reason that inspection would interfere with an active investigation. If access is denied, the Chief of Police *must provide a prompt, written denial to the requestor with* a short description of the compelling reason that access was denied. The written denial must also provide notice that relief may be sought from the district court pursuant to Minnesota Stat. §13.82, subd. 7.

g. **Death resulting from force—release of data to the public.** When an individual dies as a result of force used by an officer of this agency, all BWC data documenting the incident, redacted only as required by law, must be released and classified as public within 14 days after the incident, unless the Chief of Police asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remains classified by Minnesota Stat. §13.82, subd. 7.

h. **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.

i. **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, using an external device to screen record BWC data and share to others via text or other means.

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 external law enforcement training purposes must be approved by the Chief of Police and/or their designee. BWC footage used for external law enforcement training purposes shall be redacted prior to use. Field training officers and supervisors may review BWC data with officers for the purpose of providing coaching and feedback on the officer's performance. This may include reviewing BWC data at team musters with the sole and documented purpose of internal departmental training. The documentation shall be done in the notes section of the BWC data with a description of the purpose of the training review.

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.

j. **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.

G. 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.

H. Agency Use of Data

a. All relevant BWC recordings related to Use of Force and Vehicle Pursuits will be reviewed and documented as part of the supervisory review of these incidents.

b. Every month, 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. This review will include a minimum of two BWC videos created by each officer. The videos selected for the monthly review will not include Test/Accidental recordings/Non-Evidentiary Citizen Contacts, or videos that have been reviewed due to a Use of Force or pursuit related incident.

c. In addition, a supervisor and other assigned personnel may access BWC data to review officer performance, or investigate a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

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

e. 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.

I. 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. All BWC data documenting a peace officer using deadly force must be maintained indefinitely.

c. 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.

d. 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.

e. 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.

f. Subject to part g (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.

g. 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.

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

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

APPENDIX B:

ST. CLOUD POLICE DEPARTMENT
Law Enforcement
Policies and Procedures

Subject: Body Worn Cameras (BWC)	Policy Number: 235
Issue Date: 02-02-2021	Revision Date: 05-21-24; 06-04-24; 11-22-24; 12-09-24
Approval Authority - Title and Signature: Jeffrey Oxton, 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
Minn. Stat. §626.8473 and Minn. Stat. §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:

L. **Body Worn Camera (BWC)** 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.

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

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

O. **UMD** refers to Until Manually Deleted relating to the storage of BWC recordings in Axon Evidence.

P. **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.

Q. **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.

R. **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.

S. **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.

T. **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, BWC function test, recordings made in station house locker rooms, and 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.

U. **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's 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.

V. **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

J. 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. A function test shall consist of the operator undocking the BWC, activating then stopping a recording to confirm the device is working 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 assigned a BWC shall wear and operate the system in compliance with this agency's policy while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official.

d. When BWC's are required to be worn, all officers ~~in uniform~~, to include officers wearing any type of outer tactical vest carrier, ~~who are required to wear a BWC~~, shall 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 footage of the officer's activities. The mid-line of the waist will be one inch above the officer's navel.

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

3. Whenever an officer makes a recording relating to a CFS, the existence of the recording shall be documented in an incident report or Computer-Aided Dispatch (CAD) record of the event. An exception to this requirement would be recordings that are test/accidental/non-evidentiary citizen contacts in nature.

4. 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.

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

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

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

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

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

K. General Guidelines for Recording

a. Officers shall activate their BWCs while responding to all calls for service prior to arriving on scene and interacting with those involved in the respective incident (whether in person or via phone), 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 in the General Guidelines for Recording, part a (above), officers have the discretion to record or not record general citizen contacts, contracted overtime activities, and extra or directed patrols.

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.

L. 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.

M. Livestreaming BWC video utilizing WatchMe

a. WatchMe is a livestreaming feature that allows the end operators to initiate a request for an authorized user to livestream the operator's actively recording BWC video and audio.

1. Authorized users that receive the request and have the ability to livestream BWC video and audio will be Sergeants, Lieutenants, Commanders, Assistant Chief of Police, and the Chief of Police.

2. This policy does not mandate the use of the WatchMe feature by the end operator, nor does it mandate an authorized user to accept the request and livestream the BWC video and audio.

3. In limited circumstances, a supervisor can direct an officer to activate the WatchMe feature while on an active call for service which may necessitate supervisor response or guidance and physical response cannot readily be achieved. This does not replace the need for a supervisor to respond to the scene when able to do so. This type of directive will require the supervisor to notify their chain of command via email and provide a brief explanation of the situation, and the need for the directive.

N. 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 to Axon Evidence.

b. Officers shall accurately label the BWC data files at the time of capture, or prior to the 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 category labels as are applicable to each file:

Category Label	Definition	Retention	Category Duration
1-Test/Accidental/CC	Test/Accidental Activation/Non-Evidentiary Citizen Contact	See Category Duration	90 Days
No Report	Call for Service cleared in CAD/Traffic Stop/Crash No Citation/General Citizen Contact/Adversarial Contact/Transport	See Category Duration	1 Year
Report-RMS	RMS Report completed/Citation Issued/ Arrest Made	See Record Retention Schedule*	UMD
Discharge of Firearm	By a Peace Officer in the Course of Duty, other than for Training Purposes or the Killing of an Animal that is Sick, Injured, or Dangerous	1 Year	1 Year
Use of Force/Fleeing	Use of Force/Fleeing	See Record Retention Schedule	7 Years
Internal Investigations	Internal Investigation	See Record Retention Schedule **	UMD
Formal Complaint	Formal Complaint Made Against Peace Officer	See Record Retention Schedule	1 Year
Death/CSC	Death/Criminal Sexual Conduct Investigation	See Record Retention Schedule	UMD
Specialty/Restricted	VOTF/CMHTTF/SWAT	See Record Retention Schedule	7 Years

* Data will be manually deleted after final case disposition, or statute of limitations has expired
** 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.

O. 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 Minn. Stat. §13.82, subd. 15.

f. **Death resulting from force—access to data by survivors and legal counsel.** Notwithstanding any other law or policy to the contrary, when an individual dies as a result of force used by an officer of this agency, all BWC data documenting the incident, redacted only as required by law, must be made available for inspection by any of the following individuals within five days of their request:

1. The deceased individual's next of kin;

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

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

The request may be denied if there is a compelling reason that inspection would interfere with an active investigation. If access is denied, the Chief of Police *must provide a prompt, written denial to the requestor with* a short description of the compelling reason that access was denied. The written denial must also provide notice that relief may be sought from the district court pursuant to Minnesota Stat. §13.82, subd. 7.

g. **Death resulting from force—release of data to the public.** When an individual dies as a result of force used by an officer of this agency, all BWC data documenting the incident, redacted only as required by law, must be released and classified as public within 14 days after the incident, unless the Chief of Police asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remains classified by Minnesota Stat. §13.82, subd. 7.

h. **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.

i. **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, using an external device to screen record BWC data and share to others via text or other means.

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 external law enforcement training purposes must be approved by the Chief of Police and/or their designee. BWC footage used for external law enforcement training purposes shall be redacted prior to use. Field training officers and supervisors may review BWC data with officers for the purpose of providing coaching and feedback on the officer's performance. This may include reviewing BWC data at team musters with the sole and documented purpose of internal departmental training. The documentation shall be done in the notes section of the BWC data with a description of the purpose of the training review.

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.

j. **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.

P. 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 data or metadata ~~unless otherwise expressly authorized by the Chief of Police and/or their designee~~. This does not include an officer's ability to correct errant BWC metadata, including but not limited to corrections to the original metadata entry(s) that were entered incorrectly.

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.

Q. Agency Use of Data

a. All relevant BWC recordings related to Use of Force and Vehicle Pursuits will be reviewed and documented as part of the supervisory review of these incidents.

b. Every month, 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. This review will include a minimum of two BWC videos created by each officer. The videos selected for the monthly review will not include Test/Accidental recordings/Non-Evidentiary Citizen Contacts, or videos that have been reviewed due to a Use of Force or pursuit related incident.

c. In addition, a supervisor and other assigned personnel may access BWC data to review officer performance, or investigate a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

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

e. 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.

R. 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. All BWC data documenting a peace officer using deadly force must be maintained indefinitely.

c. 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.

d. 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~~ that requires a use of force report or supervisory review.

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

e. 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.

f. Subject to part g (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.

g. 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.

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

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