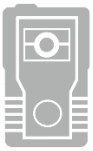
INDEPENDENT AUDITOR'S REPORT

Mankato Department of Public Safety



APRIL 9TH, 2025

RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear Mankato City Council and Public Safety Director Clifton:

We have audited the body-worn camera (BWC) program of the Mankato Department of Public Safety (MDPS) for the two-year period ended 10/21/2024. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)[1] program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Mankato Department of Public Safety. Our responsibility is to express an opinion on the operations of this program based on our audit.

On January 24, 2025, Rampart Audit LLC (Rampart) met with Commander Justin Neumann and Records Supervisor Kay Schultz both of whom provided information about MDPS' 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 MDPS' recordkeeping.

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

MDPS BWC Program Implementation and Authorization

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

> A local law enforcement agency must provide an opportunity for public comment before it purchases or implements a portable recording system. At a minimum, the agency must accept public comments submitted electronically or by mail, and the governing body with jurisdiction over the budget of the law enforcement agency must provide an opportunity for public comment at a regularly-scheduled meeting.

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

MDPS personnel advised us that their BWC program was implemented on 10/17/2022. MDPS provided the following documentation to show that the public notice and hearing requirements were met prior to the program's implementation:

- A copy of a memo, dated March 23, 2022, from Mankato City Manager Susan Arntz to the Mankato City Council, providing a history of the proposed BWC program, beginning in June of 2021, as well as a summary of 72 responses received via phone, email and an online poll, indicating overwhelming community support for the proposed purchase of BWCs. The memo included an acquisition plan and timeline to proceed with the implementation process.
- A copy of a memo, dated April 4, 2022, from City Manager Arntz to the Mankato City Council, establishing a timeline and a list of action items to complete prior to the implementation of MDPS' BWC program. The list includes:
    - an announcement of the proposal at the April 11, 2022, Mankato City Council Meeting;
    - a month-long solicitation of online comments through the Every Voice Mankato website; and
    - a public hearing to receive in-person comments at the May 9, 2022, Mankato City Council meeting.
    - The memo also includes the text of §626.8473 Subd. 3, which sets forth the requirements of a BWC policy.
    - In addition to the online comment option, the memo includes phone and email contact information, as well as a physical mailing address for those wishing to provide comments in another form.
    - Finally, the memo contained the text of the proposed BWC policy.
- A summary of the more than two dozen comments received from the public via phone, email and online regarding the proposed BWC program and policy.

Copies of these documents have been retained in Rampart's audit files. In our opinion, MDPS satisfied the requirements of §626.8473 Subd. 2 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."

Rampart verified that there was a working link to MDPS' BWC policy on the Public Safety Dashboard of the City of Mankato's website. In our opinion, Mankato Department of Public Safety is compliant with the requirements of §626.8473 Subd. 3(a).

MDPS BWC WRITTEN POLICY

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

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

1) The requirements of section 13.825 and other data classifications, access procedures, retention policies, and data safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;
2) A prohibition on altering, erasing or destroying any recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely;
3) A mandate that a portable recording system be worn at or above the mid-line of the waist in a position that maximizes the recording system's capacity to record video footage of the officer's activities;
4) A mandate that officers assigned a portable recording system wear and operate the system in compliance with the agency's policy adopted under this section while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official;
5) A mandate that, notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the deceased individual's next of kin, the legal representative of the deceased individual's next of kin, and the other parent of the deceased individual's child, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, with the following exception:
    a) A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to section 13.82 subdivision 7;
6) A mandate that, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82 subdivision 7;
7) Procedures for testing the portable recording system to ensure adequate functioning;
8) Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
9) Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
10) Circumstances under which a data subject must be given notice of a recording;
11) Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
12) Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
13) Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

In our opinion, the MDPS 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.

MDPS BWC Data Retention

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

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

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

The Data Retention section of MDPS' BWC policy states that: "[a]ll BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data." This section also includes the required retention period for each of the individual data categories listed above.

In our opinion, MDPS' BWC policy meets the retention requirements contained in Minn. Stat. §13.825 Subd. 3.

The Data Security Safeguards section of MDPS' BWC policy states that:

> The video storage database shall be administered in a manner that prevents users from editing, altering, or erasing any BWC recording unless expressly authorized by the Director of Public Safety or their designee. Officers and civilian employees shall not intentionally erase, alter, modify, or tamper with BWC data or metadata. Only a supervisor, BWC administrator, BWC technician, or other approved designee, may erase media in accordance with this policy.

Taken in conjunction with the mandatory language contained in the retention periods described above, it is our opinion that MDPS' BWC policy satisfies the requirement described in Clause 2 of the Policy section of this report that a BWC policy prohibit altering, erasing or destroying BWC data prior to its scheduled expiration date; however, we recommend adding language to state explicitly that no BWC data or metadata may be deleted prior to the expiration of the associated retention period.

MDPS employs Axon 3 body-worn cameras and utilizes Axon's Cloud Service storage (Evidence.com) and 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 by the DPS Director, Deputy Director,

Commander or the Records supervisor as needed. If an officer fails to assign a data classification, the default retention period is indefinite to avoid the accidental loss of data.

MDPS' BWC policy states that:

> Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from their BWC to Evidence.com by the end of their 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.

The policy further states that "[o]fficers shall classify the BWC data files at the time of video capture or transfer to storage…"

Commander Neumann advised that the Axon body-worn cameras utilize physical docking stations located at the Mankato Department of Public Safety.

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

MDPS BWC Data Destruction

As discussed above, MDPS utilizes Axon's Evidence.com for storage, with retention periods determined based on the classification assigned to BWC data. BWC recordings are purged automatically within Evidence.com upon expiration of the associated retention period.

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

FBI CJIS policy requires that hard drives used for CJIS data storage are sanitized by overwriting at least three times or degaussing prior to being released to unauthorized individuals, while inoperable drives must be destroyed through physical means such as shredding.

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

MDPS BWC Data Access

The Access to BWC Data by Non-Employees section of MDPS' BWC policy states that:

> Officers shall refer members of the media or public seeking access to BWC data to the Mankato Department of Public Safety Records Department, who shall process the request in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws.

Commander Neumann advised us that that all requests for BWC data from the public or media are made in writing using Mankato Department of Public Safety's data request form. Requests are processed by Records staff. BWC video is provided to members of the public via physical media such as DVD or USB memory device.

As discussed in Clauses 5 and 6 of the Policy section of this report, the Minnesota State Legislature in 2023 added specific access requirements related to BWC data that document deadly force incidents, and specified that these requirements must be included in the agency's BWC policy. A review of the Access to BWC Data in Incidents of Death as a Result of Force by a Peace Officer section of MDPS' BWC policy shows that MDPS has incorporated these requirements into its BWC policy.

MDPS' BWC policy states that "BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure." Requests for BWC data from other law enforcement agencies are submitted via email to the Records department, and must include the purpose and intended use of the data. Commander Neumann advised us any record clerk can receive the request, but Kay Schultz is the one who receives and processes the requests. BWC data are shared with other law enforcement agencies via email containing a secure Evidence.com internet link.

In addition, the policy states that "BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law." Prosecutors have direct, read-only access to MDPS' Evidence.com data.

MDPS advised us that BWC recordings are only shared with other agencies that have BWC programs and are therefore presumed to have appropriate policies and safeguards in place. Commander Neumann indicated that MDPS also currently has a memo of obligation attached regarding the receiving agency's obligations under §13.825 Subd. 7 and Subd. 8, which include a requirement to maintain BWC data security. Rampart advised a written acknowledgement or agreement is recommended with departments receiving MDPD BWC data. Prior to the issuance of this report Commander Neumann also advised that MDPD was now going to utilize a template from a neighboring law enforcement organization to receive signed obligations under 13.825 Subd. 7 & Subd. 8. Rampart has direct knowledge and copies of this document in our files.

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

MDPS BWC Data Classification

MDPS' BWC Policy states that:

> BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result, BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.

Active criminal investigation data are classified as confidential. MDPS BWC Policy also identifies certain categories of BWC data that are public.

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

In our opinion, MDPS' written BWC policy is compliant with respect to the applicable data classification requirements.

MDPS BWC Internal Compliance Verification

The MDPS BWC Compliance section states that "[s]upervisors shall monitor for compliance with this policy," but does not identify a process for doing so. MDPS advised us that supervisors do conduct random reviews of BWC recordings, and that these reviews are recorded in the Axon Performance audit trail system. Minn. Stat. §626.8473 Subd. 12 requires that a BWC policy include "procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews…"

While it is our opinion that MDPS is compliant with the supervisory review requirement in practice, Rampart recommends that MDPS add language to their BWC policy requiring supervisors to conduct reviews or internal audits on a regular basis. All access to BWC data is logged in the Axon Evidence software, and supervisory reviews should include monitoring of such access.

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

As discussed in Clause 4 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must require that an officer assigned a BWC wear and operate the system in compliance with the agency's BWC policy while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official. The Use and Documentation section of MDPS' BWC policy includes language to address this new requirement: "Officers assigned a BWC must wear and operate the BWC in compliance with this policy while performing activities under the command and control of another chief law enforcement officer or federal law enforcement official."

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

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

MDPS BWC Program and Inventory

MDPS currently possesses 64 Axon 3 body-worn cameras, including 10 held as spares.

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

As discussed in Clause 3 of the Policy section of this report, the 2023 legislative changes require that an agency's BWC policy must specify that a BWC be worn at or above the mid-line of the waist. The LEO Responsibilities section of MDPS' BWC policy states:

> Officers are required to wear their issued BWCs in the manner specified in training. BWCs must be worn in a forward-facing position 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.

While all MDPS officers are issued BWCs, the policy identifies certain personnel such as investigators who are given discretion with regard to their use, except in cases of planned enforcement activities, where usage is mandatory. In our opinion, the language above satisfies the requirement that, whenever BWC usage is required, officers are instructed to wear the device at or above the mid-line of the waist.

Commander Neumann advised us that he is able to determine the number of BWCs deployed by reviewing the schedule and/or payroll data, as well as by monitoring the Axon Respond application, which provides real-time location data.

As of 2/06/2025, MDPS maintained 55,578.7 GB of BWC data.

MDPS BWC Physical, Technological and Procedural Safeguards

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

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes, as well as the ability to add or edit case numbers and titles. All BWC data access is logged automatically and available for audit purposes.

Enhanced Surveillance Technology

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

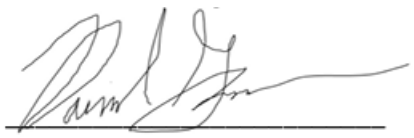
If MDPS should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses.

Data Sampling

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

Audit Conclusions

In our opinion, the Mankato Department of Public Safety's Body-Worn Camera Program is substantially compliant with Minnesota Statutes §13.825 and §626.8473.



Rampart Audit LLC

4/09/2025

APPENDIX A:

Policy
424

Mankato Department of Public Safety

Mankato Dept of PS Policy Manual

Portable Audio/Video Recorders

424.1 PURPOSE AND SCOPE

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

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad-car based (dash cam) recording systems. The Director, or their designee, may supersede this policy by providing specific instructions for BWC use to individual officers, providing specific instructions pertaining to a particular event or classes of events, or provide specific instructions or standard operating procedures for BWC use to officers assigned to specialized details.

424.1.1 DEFINITIONS

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

Activation - Any process that causes BWC system to record audio or video data. Activation can only occur when the BWC is already powered on.

Adversarial - 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.

Classify - Refers to an event that has been recorded and for which a predetermined retention

period has been set.

Deactivation - Any process that causes the BWC system to stop recording. Deactivation can be done manually or can occur accidentally

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.

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

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

MGDPA or Data Practices Act - Refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq.

Official duties - Means that the officer is on-duty, or working in an off-duty capacity for the City of Mankato, and performing authorized law enforcement services on behalf of this agency.

PODPA- The Peace Officer Discipline Procedures Act, Minnesota Statutes Section 609.89.

Records Retention Schedule - Refers to the General Records Retention Schedule for Minnesota Cities.

Unintentionally recorded footage - A video recording that results from an officer's inadvertence 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.

424.2 POLICY

It is the policy of this department to authorize the use of department issued (BWCs) as set forth below, and to administer BWC data as provided by law. Sworn officers who have been issued BWCs shall use them consistent with this policy.

424.3 USE AND DOCUMENTATION

Uniformed officers who are working patrol, traffic enforcement, special details, or department authorized off-duty details must be equipped with a BWC unless permission has been granted by a supervisor to deviate from this policy. Officers working administrative assignments are not required to be equipped with a BWC but may elect to use a BWC pursuant to the needs of a specific investigation or job duty. Officers assigned a BWC must wear and operate the BWC in compliance with this policy while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official.

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. Officers shall not use their BWC to record non-work- related activity.

Officers who have been issued BWCs must operate and use them consistent with this policy. Officers must 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 must promptly report the malfunction to the officer's supervisor. Supervisors should take prompt action to address malfunctions, assign spare equipment when necessary, and report malfunctions to appropriate staff, and document the steps taken in writing.

Prior to utilizing BWCs, users shall complete an approved training course covering proper operation of assigned equipment and a review of this policy. Officers are required to wear their issued BWCs in the manner specified in training. BWCs must be worn in a forward-facing position

at or above the midline of the waist in a position that maximizes the recording system's capacity to record video footage of the officer's activities.

Officers must document BWC use, and non-use as follows:

1. Whenever an officer makes a recording, the existence of the recording will be documented in an incident report. If no report is written, it should be documented in the records management system

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. If no incident report is written, it should be documented in the records management system. Supervisors shall review these reports and initiate any corrective action deemed necessary. If an activity was not recorded due to a supervisor directive, the circumstances shall be documented in the same manner.

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 department
2. A daily record of the total number of BWCs deployed and used by officers
3. The total amount of recorded BWC data collected and maintained
4. This policy, together with the Records Retention Schedule

424.4 GENERAL GUIDELINES FOR RECORDING

Officers shall activate their BWCs when they anticipate participating in an activity likely to yield information having evidentiary value. Situations that qualify include, but are not limited to; a pursuit, Terry Stop of a motorist or pedestrian, search, seizure, arrest, use of force, or adversarial contact. However, officers are not required to activate their cameras when it would be unsafe, impossible, or impractical to do so. Such instances of not recording when otherwise required must be documented as specified in the Use and Documentation section of this policy.

Officers have discretion to record or not record general citizen contacts. 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.

Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded. However, if asked, officers shall advise citizens they are being recorded.

Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene may direct the discontinuance of

recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued or muted while an investigation, response, or incident is ongoing, officers shall state the reasons for ceasing the recording on camera before deactivating their BWC. If circumstances change, officers shall reactivate their cameras as required by this policy to capture information having evidentiary value.

Officers shall be sensitive to the dignity of members of the public being recorded and exercise sound discretion to respect privacy by discontinuing recording when it reasonably appears that such privacy outweighs any legitimate law enforcement interest in recording. Requests by members of the public to stop recording should be considered using these same criteria. Recording should resume when privacy is no longer at issue unless no longer required by another section of this policy. Officers must state the reason on camera before deactivating their BWC and specify the circumstances in their report.

Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of 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, in restrooms, during breaks, or during other private conversations or within areas of the Public Safety Center restricted to personnel-only unless recording is authorized as part of an administrative or criminal investigation.

424.4.1 SPECIAL ASSIGNMENTS

Personnel assigned to covert/undercover assignments do not need to wear their BWC during operations in which displaying or indicating their status as an officer would compromise the operation. Officers serving in a special assignment role must make a reasonable effort to have their BWCs with them throughout their course of duty.

Officers assigned to the Detective Division as Detectives shall activate their BWCs during the following situations:

1. When at an active scene where recording is likely to yield information having evidentiary value.
2. When executing a search warrant outside of a controlled facility or environment until the scene is secured or it becomes apparent that additional recording is unlikely to capture information having evidentiary value. (e.g., Detectives do not need to activate their BWC when executing a financial records warrant at a financial institution, but would at all residences and other similar environments.)
3. During the interview of a suspect when other means of recording are not available.

Officers serving as an agent of the MRVDTF shall activate their BWCs during the following situations:

1. Prior to any enforcement action, when feasible, without jeopardizing agent safety (e.g., execution of search warrants, reasonably anticipated pre-planned events, assisting on an active call for service, etc.)

Officers actively serving as a member of the MRVTRT in response to a team activation or callout, shall activate their BWCs during the following instances:

1. Upon arrival to the outer perimeter of the scene and throughout the operation until the location is secured (e.g., a TRT assisted search or arrest warrant). For extended tactical operations, recording will begin when the officer is deployed to the scene and should capture any negotiations and other relevant activity when possible. Recording should continue until the incident is resolved or the member is relieved from the active scene and transitioned to a standby role.

Officers assigned as an SRO shall follow the General and Special Guidelines for recording.

424.4.2 SPECIAL GUIDELINES FOR RECORDING

Officers may, in the exercise of sound discretion, determine 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. Officers may also use their BWCs, or Axon Capture, to take recorded statements from persons believed to be victims of and witnesses to crimes, and persons suspected of committing crimes, considering the needs of the investigation and the circumstances pertaining to the victim, witness, or suspect.

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

Officers shall use their BWCs and squad-based audio/video systems to record their transportation and the physical transfer of persons in their custody to hospitals, detox, mental health care facilities, shelters, advocacy centers, 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.

Officers should not activate their BWCs during court appearances, while waiting for court appearances in the Justice Center, or in Judge's chambers. Officers shall activate their BWCs in the courtrooms or Justice Center if they anticipate that they will be involved in or become involved in a pursuit, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value, or with the express permission of the presiding judge.

Officers should make best efforts to avoid recording law enforcement restricted data on a BWC that may be verbal, written, or electronic format. Examples include, but are not limited to: computer screen or Driver's Licenses, school, or medical information.

424.5 DOWNLOADING AND CLASSIFYING DATA

Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from their BWC to Evidence.com by the end of their 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.

Officers shall classify 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 classification. If multiple classifications apply to the BWC data, officers may classify the recording with multiple classification categories.

Classifications and retention periods for BWC data are as follows:

1. **Evidence:** The recording has evidentiary value with respect to an actual or suspected criminal incident or involved an adversarial encounter that could result in a complaint against an officer. (Retention duration: 30 years)

2. **Non-enforcement contact:** The recording does not fit into any other category and has no apparent evidentiary value including recordings of general citizen contacts. (Retention duration: 90 days)

3. **Non-traffic citation, arrest, LOT:** The recording involves enforcement that ended in a citation, physical arrest, or request to prosecutors for criminal charges. (Retention duration: 30 years)

4. **Officer injury:** The recording involves an officer sustaining an injury during a recorded incident. (Retention duration: 30 years)

5. **Test/error:** Equipment testing or unintentional recordings that have no evidentiary value. (Retention duration: 90 days)

6. **Traffic citation:** Traffic related contacts when a citation is issued. (Retention duration: 1 year)

7. **Transport:** Custodial and non-custodial transports not categorized as "Arrest or Use of Force". (Retention duration: 90 days)

8. **Use of Force:** The recording involves the use of force by an officer involved in the recorded incident. (Retention duration: 7 years)

9. **Administrative:** The recording is restricted to review by command staff only. (Retention duration: Until manually deleted)

10. **Deadly Force:** The recording of a peace officer using deadly force. (Retention duration: Indefinitely)

424.6 ADMINISTERING ACCESS TO BWC DATA

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.

BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result, BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.

BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the private and/or public classifications.

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. 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.
5. Data that may aid in the law enforcement process, promote public safety, or dispel widespread rumor or unrest.

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.

424.6.1 ACCESS TO BWC DATA BY NON-EMPLOYEES

Officers shall refer members of the media or public seeking access to BWC data to the Mankato Department of Public Safety Records Department, who shall process the request 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 if the data was collected or created as part of an active investigation. Access shall not be granted to portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as potions 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, subject to redaction. Data on other individuals in the recording who do not consent to the release, or data that would identify undercover officers, must be redacted. 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.

424.6.2 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. Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Officers may review video footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident. Agency personnel shall document their reasons for accessing stored BWC data within Evidence.com at the time of each access.

Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites. Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.

424.6.3 DATA SECURITY SAFEGUARDS

Data collected via BWC will be stored on a secure system called "Evidence.com" which is cloud-based storage securely maintained by Axon. BWC data will be coded appropriately into data types and stored according to retention lengths outlined in this policy. Each officer will have a secure account assigned to them through Evidence.com to manage data they have collected. The Director of Public Safety, and their designee(s), will have administrator capabilities for the purpose of managing and reviewing data. Prosecuting law attorneys will also be granted secure access to Evidence.com for the purposes of viewing specific evidentiary data necessary for prosecution and discovery.

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

The video storage database shall be administered in a manner that prevents users from editing, altering, or erasing any BWC recording unless expressly authorized by the Director of Public Safety or their designee. Officers and civilian employees shall not intentionally erase, alter, modify, or tamper with BWC data or metadata. Only a supervisor, BWC administrator, BWC technician, or other approved designee, may erase media in accordance with this policy.

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

424.6.4 AGENCY USE OF DATA

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

Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. All requests for BWC footage for training purposes should be made to the Director of Public Safety or their designee. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Police training officers (PTOs) may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

Officers and supervisors should enter notes in Evidence.com documenting why digital evidence is being accessed (e.g., "Report Writing", "Court prep", "Pursuit review", "Routine audit", "Case investigation", "Training", etc.)

424.6.5 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 shall seek supervisory approval prior to displaying video to witnesses and 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 screen shots, muting the audio, or playing the audio but not displaying video.

In addition, BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

424.6.6 DATA RETENTION

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

BWC data must be maintained for at least one year and destroyed according to the Records Retention Schedule if:

1. The data documents the discharge of a firearm by a police officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.
2. The data documents the use of force by a police officer that results in substantial bodily harm.
3. The data documents circumstances giving rise to a formal complaint against the officer.

Data documenting the use of deadly force by a peace officer must be maintained indefinitely in its full, unedited and unredacted state.

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. 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.

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.

The department shall maintain an inventory of BWC recordings having evidentiary value.

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

424.6.7 ACCESS TO BWC DATA IN INCIDENTS OF DEATH AS A RESULT OF FORCE BY A PEACE OFFICER

When an individual dies as a result of force used by a peace officer, The police department will allow, upon request, the following individuals to inspect all BWC data, redacted to the extent required by law, within five days of the request:

1. The deceased individual's next of kin.
2. The legal representative of the individual's next of kin
3. The other parent of the deceased individual's child.

The Mankato Department of Public Safety reserves the right to deny a request to inspect BWC data if the agency determines a compelling reason that the inspection would interfere with an active investigation. If the request is denied, the Director of Public Safety shall 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 Minn. Stat. § 13.82, subd. 7.

When an officer dies as a result of use of force by an officer, the Mankato Department of Public Safety shall release all BWC portable recording system data (redacted to the extent necessary under law), documenting the incident no later than 14 days after the incident; Unless the Director of Public Safety asserts in writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by Minn. Stat. § 13.82, subd. 7.

424.7 COMPLIANCE

Supervisors shall monitor for compliance with this policy. If an employee misuses the data covered by this policy or intentionally fails to comply with or violates this policy, it will be considered misconduct and such behavior may be grounds for disciplinary action up to and

including discharge and criminal penalties pursuant to Minn. Stat § 13.09. Any complaints of misconduct surrounding the Mankato Department of Public Safety will be investigated on a case-by-case basis, pursuant to applicable collective bargaining agreements, MN police officer discipline procedures act (Minn Stat §626.89) and department policy.

The Director of Public Safety, or their designee, shall periodically review the efficacy of the body worn camera program including review of this policy to assure it remains compliant with relevant laws and best practices.