



INDEPENDENT AUDITOR'S REPORT

Hawley Police Department



OCTOBER 4TH, 2023
RAMPART DEFENSE LLC
P.O. Box 23 Clearbrook, MN 56634

Audit Overview and Recommendations

Dear Hawley City Council and Chief Backlund:

We have audited the body-worn camera (BWC) program of the Hawley Police Department (HPD) for the period of 4/01/2021 - 3/31/2023. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)¹ program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Hawley Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On April 25, 2023, Rampart Defense LLC (Rampart) met with Chief Joe Backlund, who provided information about HPD'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 HPD's recordkeeping.

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

HPD BWC Program Implementation and Authorization

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

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

Chief Backlund provided the following document as evidence that HPD had met these requirements:

1. A screenshot of a post from Hawley Police Department's Facebook page dated 9/29/2020, which announced publicly HPD's plans to implement a BWC program. The post provided an internet link to the proposed policy, as well as information about the camera system HPD intended to purchase. It also contained an announcement that a public hearing would be held at 6:00 P.M. on 10/26/2020 at the Hawley City Council Chambers and invited the public to provide feedback either in writing in advance of the hearing or in person at the hearing.

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

2. The October 26, 2020, Hawley City Council Meeting Minutes, which note the opening of a public hearing during the regularly-scheduled city council meeting for the purpose of discussing the proposed BWC policy and program. The minutes note that the proposed BWC policy was presented, along with a discussion of the proposed body-worn cameras to be purchased, and Chief Backlund read three email comments received from the public, all of which were in favor of the BWC program.

Rampart also located multiple news reports in local media announcing the program and inviting the public to attend the public hearing or submit written comments to Chief Backlund.

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

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

Chief Backlund furnished Rampart a link to HPD's BWC policy, which was posted on the Hawley Police Department's website. Rampart verified that this link worked at the time of receipt. In our opinion, Hawley Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

HPD BWC WRITTEN POLICY

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

Prior to the issuance of this report, Chief Backlund advised us that he had adopted a new BWC policy to address various procedural and compliance issues identified during the audit. Rampart has incorporated a review of this new policy into our audit. We will identify the two policies as "Original" and "Revised" to differentiate them for purposes of this report. A copy of the revised policy is attached to this report as Appendix B.

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

1. The requirements of section 13.825 and other data classifications, access procedures, retention policies, and data safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;
2. Procedures for testing the portable recording system to ensure adequate functioning;
3. Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
4. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
5. Circumstances under which a data subject must be given notice of a recording;
6. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;

7. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
8. Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

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

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

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

HPD BWC Data Retention

Paragraph A of the Data Retention section of the HPD Original BWC policy states that “[e]videntiary data shall be retained for the period specified in the General Records Retention Schedule for Minnesota Cities. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable retention period.”

Paragraph C of the Data Retention section of the HPD Original BWC policy states that “BWC footage that is classified as non-evidentiary, or becomes classified as non-evidentiary, shall be retained for a minimum of 90 days following the date of capture...”

Paragraph B of the Data Retention section of the HPD Original BWC policy states that “[u]nintentionally recorded footage shall not be retained.” In addition, Item B.5 of the Downloading and Labeling Data section states that “[f]ootage captured through unintentional activation will be deleted at the end of the officer shift.” Paragraph E of the Data Retention section, however, includes a retention schedule that specifies a 90-day retention period for accidental recordings.

Minnesota Statute §13.825 Subd. 3(a) states that “[p]ortable recording system data that are not active or inactive criminal investigative data and are not described in paragraph (b) must be maintained for at least 90 days and destroyed according to the agency’s records retention schedule...”

Chief Backlund advised Rampart that Hawley PD follows the 90-day retention period for accidental or unintentional recordings specified in Paragraph E of the Data Retention section, and that notwithstanding the other policy entries noted above, all BWC recordings are retained for at least 90 days.

We strongly recommend that Hawley PD remove Item B.5 of the Downloading and Labeling Data section and Paragraph B of the Data Retention section, as both are substantially non-compliant with the statutory requirement that an agency retain all BWC data for a minimum of 90 days.

Minnesota Statute §13.825 Subd. 3(b) specifies a minimum retention period of one year for BWC data that document the following:

1. “[T]he discharge of a firearm by a peace officer in the course of duty if a notice is required under section 626.553 subdivision 2”; or

2. “[T]he use of force by a peace officer that results in substantial bodily harm”; or
3. “[A] formal complaint... made against the officer.”

In addition, §13.825 Subd. 3(c) requires that:

If a subject of the data submits a written request to the law enforcement agency to retain the recording beyond the applicable retention period for possible evidentiary or exculpatory use related to the circumstances under which the data were collected, the law enforcement agency shall retain the recording for an additional time period requested by the subject of up to 180 days and notify the requester that the recording will then be destroyed unless a new request is made under this paragraph.

As noted above, Hawley PD follows the General Records Retention Schedule for Minnesota Cities with respect to BWC data that are evidentiary in nature. The GRRSMC sets forth retention periods that meet or exceed the requirements for each category of BWC data enumerated in §13.825 Subd. 3(b) and (c).

HPD employs Watchguard V300 body-worn cameras and utilizes Motorola’s² VideoManager EL (Evidence Library) cloud storage service. HPD manages BWC data retention through automated retention settings in Watchguard’s Evidence Library 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.

HPD’s Original 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 by docking the unit at the end of that officer’s shift.” This is accomplished by physically docking the BWC either in the officer’s squad or at the Hawley Police Department in order to upload the data via a wireless connection. 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, HPD’s Original BWC policy is compliant with respect to the applicable data retention requirements, except for the entry in Paragraph B of the Data Retention section noted above that states “unintentionally recorded footage shall not be retained,” and the entry in the Downloading and Labeling Data section that states that “[f]ootage captured through unintentional activation will be deleted at the end of the officer shift.”

The Data Retention section of HPD’s Revised BWC policy deletes the non-compliant passages noted in the preceding paragraph and states that: “[a]ll BWC’s data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.” The revised policy also addresses the specific requirements of §13.825 Subd. 3(b), requiring a minimum retention period of one year for BWC data involving a reportable firearms discharge, and a minimum retention period of six years for data involving any use of deadly force, or force of a sufficient type or degree to require a use of force report or supervisory review; as well as any BWC data documenting circumstances that have given rise to a formal complaint against an officer. The Revised policy also contains language addressing the additional retention requirement upon receipt of a written request by a data subject.

² Motorola Solutions, Inc. acquired WatchGuard, Inc. in 2019. While Motorola is the corporate parent, both names are commonly used interchangeably in reference to the company’s mobile video products and services.

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

HPD BWC Data Destruction

As discussed above, HPD's BWC data are stored on WatchGuard's cloud-based service, with data retention and deletion schedules managed automatically through the Evidence Library video management software based on the assigned data classification of each video.

WatchGuard utilizes Microsoft's Azure Government environment for cloud storage. Microsoft certifies this environment as being compliant with the current Federal Bureau of Investigation Criminal Justice Information Services Division Security Policy (5.9.2), and notes that it has signed CJIS management agreements with 45 of the 50 U.S. states, including Minnesota, to verify compliance with state CJIS requirements.

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

HPD BWC Data Access

HPD's Original BWC policy states that officers shall refer "members of the media or public seeking access to BWC data to the Hawley Police Department Records Division, who will process the request in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws." BWC recordings are shared with members of the public via whichever form they request, typically physical media such as DVD or USB, alternatively members of the public can simply view the data at the Police Department. Such recordings are subject to redaction as described in §13.825 Subd. 4(b).

HPD's BWC policy also states that BWC data "shall be made available to prosecutors, courts, and other criminal justice entities as provided by law." Chief Backlund advised us that there is a verbal agreement in place with neighboring agencies regarding their responsibilities under §13.825 Subd. 8(b) to maintain the data classification, destruction and security requirements of §13.825 with respect to any BWC data HPD shares with those agencies. We recommend obtaining a written acknowledgement of those responsibilities.

BWC data are shared with prosecutors and other law enforcement agencies via an expiring internet link provided by email.

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

HPD's Revised BWC policy retains the data access language discussed above and, in our opinion, is also compliant with the applicable data access requirements.

HPD BWC Data Classification

Minn. Stat. §13.825 Subd. 2(a) states that data collected by a portable recording system are private data on individuals or nonpublic data, subject to certain exceptions enumerated in the statute.

HPD's Original BWC policy does not address the subject of data classification, aside from noting that requests for BWC data will be processed in accordance with the MGDPA, as discussed in the preceding section of this report.

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

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

HPD BWC Internal Compliance Verification

The HPD Original BWC policy Agency Use of Data section authorizes access of 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," but does not otherwise address supervisory reviews or internal audits to ensure compliance with the policy, nor does it address the employee discipline standards for unauthorized access to data or other violations of the BWC policy. §626.8473 Subd. 3(b)(8) mandates that any written BWC policy incorporates both of these elements.

The HPD Revised BWC policy Agency Use of Data section states that:

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

In addition, supervisors and other assigned personnel may access BWC's 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.

Chief Backlund advised us that (Per policy use of data section) he reviews several videos per officer each month.

HPD's Revised BWC policy Compliance section states that "[s]upervisors shall monitor for compliance with this policy. The unauthorized access to or disclosure of BWC's data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. §13.09."

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

HPD BWC Program and Inventory

HPD currently possesses five (5) Watchguard V300 body-worn cameras.

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

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

As of the time of the audit, HPD maintained 1,238 BWC data files.

HPD BWC Physical, Technological and Procedural Safeguards

HPD 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 either in his or her squad or at HPD. Any BWC data are then uploaded automatically to Motorola's VideoManager Evidence Library cloud storage system.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes.

Enhanced Surveillance Technology

HPD 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 HPD 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 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 auditors reviewed the retained BWC videos to determine whether this data was accurately documented in HPD records.

Rampart Defense, LLC

All reviewed videos were properly identified by CFS number.

Audit Conclusions

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



Daniel E. Gazelka

Rampart Defense LLC

10/04/2023

APPENDIX A (original policy)

Hawley Police Department Policy Manual

SECTION 27

Body Word Camera (BWC)

I. PURPOSE

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

II. POLICY

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

III. SCOPE

This policy governs the use of BWC's in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The chief or chief's designee may supersede this policy by providing specific instructions for BWC's use to individual officers, or providing specific instructions pertaining to particular events or classes of events, including but not limited to political rallies and demonstrations.

The chief or designee may also provide specific instructions or standard operating procedures for BWC's use to officers assigned to specialized details, such as carrying out duties in courts or guarding prisoners or patients in hospitals and mental health facilities

IV. DEFINITIONS

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

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

- B. Records Retention Schedule refers to the General Records Retention Schedule for Minnesota Cities.
- C. Law enforcement-related information means information captured or available for capture by use of a BWC's that has evidentiary value because it documents events with respect to a stop, arrest, search, citation, or charging decision.
- D. Evidentiary value means that the information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or officer.
- E. General Citizen Contact means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a wrecker, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.
- F. Adversarial 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.
- G. Unintentionally recorded footage is a video recording that results from an officer's inadvertence or neglect in operating the officer's Portable Recording Device, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms, restrooms, and recordings made while officers were engaged in conversations of a non-business, personal nature with the expectation that the conversation was not being recorded.
- H. Official duties, for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this agency.

V. USE AND DOCUMENTATION

- A. Officers may use only department-issued BWC's 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 BWC's shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWC's at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document

the steps taken in writing

- C. Officers should wear their issued BWC's at the location on their body and in the manner specified in training.
- D. Officers must document BWC's use and non-use as follows:
 - 1. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report.
 - 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. Supervisors shall review these reports and initiate any corrective action deemed necessary.
- E. The department will maintain the following records and documents relating to BWC's use, which are classified as public data:
 - 1. The total number of BWC's owned or maintained by the agency;
 - 2. A daily record of the total number of BWC's actually deployed and used by officers and, if applicable, the precincts in which they were used;
 - 3. The total amount of recorded BWC's data collected and maintained; and
 - 4. This policy, together with the Records Retention Schedule.

VI. GENERAL GUIDELINES FOR RECORDING

- A. Officers shall activate their BWC's when responding to all calls for service and during all law enforcement-related encounters and activities, including but not limited to pursuits, *Terry* stops of motorists or pedestrians, arrests, searches, suspect interviews and interrogations, and during any police/citizen contacts that becomes 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 documented as specified in the Use and Documentation guidelines, part (D)(2) (above).
- B. Officers have discretion to record or not record general citizen contacts.
- C. Officers have no affirmative duty to inform people that a BWC's is being operated or that the individuals are being recorded.
- D. Once activated, the BWC's should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information

having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, officers shall state the reasons for ceasing the recording on camera before deactivating their BWC's. 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 Portable Recording Device's audio or visual recording functionality to defeat the purposes of this policy.
- F. Notwithstanding any other provision in this policy, officers shall not use their BWC's 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.

VII. SPECIAL GUIDELINES FOR RECORDING

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

- A. To use their BWC's 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. To use their BWC's 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.
- C. 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, BWC's shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.
- D. Officers shall use their Portable Recording Device 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.

VIII. DOWNLOADING AND LABELING DATA

- A. Each officer using a BWC's is responsible for transferring or assuring the proper transfer of the data from his or her camera to upload to the Watchguard/Motorola system 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 or investigator shall take custody of the officer's Portable Recording Device and assume responsibility for transferring the data from it.

- B. Officers shall label the BWC's data files at the time of capture or transfer to storage, and should consult with a supervisor if in doubt as to the appropriate labeling. Officers should assign as many of the following labels as are applicable to each file:
1. Accidental Record
 2. Citizen Contact
 3. Traffic - Citation
 4. Traffic - Warning
 5. Fleeing in Motor Vehicle
 6. Traffic Inv./Other
 7. Motorist Assist
 8. Suspicious Vehicle/Behavior
 9. Test Recording
 10. Narcotics Investigation
 11. Investigation/Other
 12. Assault
 13. Medical
 14. SRO/School
- C. In addition, officers shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under the MGDPA limiting disclosure of information about them. These individuals include:
1. Victims and alleged victims of criminal sexual conduct and sex trafficking.
 2. Victims of child abuse or neglect.
 3. Vulnerable adults who are victims of maltreatment.
 4. Undercover officers.
 5. Informants.
 6. When the video is clearly offensive to common sensitivities.
 7. Victims of and witnesses to crimes, if the victim or witness has requested not to be identified publicly.
 8. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system.
 9. Mandated reporters.
 10. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness.
 11. Juveniles who are or may be delinquent or engaged in criminal acts.

12. Individuals who make complaints about violations with respect to the use of real property.
 13. Officers and employees who are the subject of a complaint related to the events captured on video.
 14. Other individuals whose identities the officer believes may be legally protected from public disclosure.
- D. Labeling and flagging designations may be corrected or amended based on additional information.

IX. ADMINISTERING ACCESS TO BWC'S DATA

- A. Data subjects. Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC's 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's data is presumptively private. BWC's recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:
1. BWC's data pertaining to people is presumed private, as is BWC's data pertaining to businesses or other entities.
 2. Some BWC's data is classified as confidential (see C. below).
 3. Some BWC's data is classified as public (see D. below).
- C. Confidential data. BWC's 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's 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. However, if another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other classification. For instance, data that reveals protected identities under Minn. Stat. § 13.82, subd. 17 (e.g., certain victims, witnesses, and others) should not be released even if it would otherwise fit into one of the public categories listed above.
- E. Access to BWC's data by non-employees. Officers shall refer members of the media or public seeking access to BWC's data to the Chief or designee, 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's 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.
- F. Access by peace officers and law enforcement employees. No employee may have access to the department's BWC's data except for legitimate law enforcement or data administration purposes:
1. Officers may access and view stored BWC's video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Except as provided in the critical incident response policy, 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.
 2. Agency personnel shall document their reasons for accessing stored BWC's data in the manner provided within the database at the time of each access. Agency personnel are

prohibited from accessing BWC's data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC's data recorded or maintained by this agency to public and social media websites.

3. Employees seeking access to BWC's data for non-business reasons may make a request for it in the same manner as any member of the public.

G. Other authorized disclosures of data. Officers may display portions of BWC's 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 screen shots, muting the audio, or playing the audio but not displaying video. In addition,

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

X. DATA SECURITY SAFEGUARDS

A. The data security safeguards will be handled by the IT personnel contracted by the City of Hawley Police Department.

B. Access to BWC's data from city or personally owned and approved devices shall be managed in accordance with established city policy.

C. Officers shall not intentionally edit, alter, or erase any BWC's recording unless otherwise expressly authorized by the chief or the chief's 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's program.

XI. AGENCY USE OF DATA

A. At least once a month, supervisors will randomly review BWC's usage by each officer to whom a BWC's is issued or available for use, to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.

- B. In addition, supervisors and other assigned personnel may access BWC's data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.
- C. Nothing in this policy limits or prohibits the use of BWC's data as evidence of misconduct or as a basis for discipline.
- D. Officers should contact their supervisors to discuss retaining and using BWC's footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training officers may utilize BWC's data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

XII. DATA RETENTION

- A. All BWC's data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.
- B. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.
- C. Certain kinds of BWC's data must be retained for six years:
 - 1. Data that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report or supervisory review.
 - 2. Data documenting circumstances that have given rise to a formal complaint against an officer.
- D. Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.
- E. Subject to Part F (below), all other BWC's footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.
- F. Upon written request by a BWC's data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. The agency will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received.
- G. The department shall maintain an inventory of BWC's recordings having evidentiary value.
- H. The department will post this policy, and the following retention rules on the City of Hawley's website <https://hawley.govoffice.com/police>
- I. Retention Rules

1. Default	90 days
2. Accidental Record	90 days
3. Citizen Contact	1095 days (3 years)
4. Traffic Citation	1095 days (3 years)
5. Traffic Warning	90 days
6. Fleeing in MV	2555 days (7 years)
7. DWI/DUI	2555 days (7 years)
8. Traffic Inv/Other	2555 days (7 years)
9. Motorist Assist	90 days
10. Suspicious Vehicle/Behavior	90 days
11. Test Recording	90 days
12. Narcotics Investigation	2555 days (7 years)
13. Investigation (Other)	2555 days (7 years)
14. Assault	2555 days (7 years)
15. Medical	90 days
16. SRO/School	90 days

XIII. COMPLIANCE

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

APPENDIX B (revised policy)

SECTION 27

Body Word Camera (BWC)

I. PURPOSE

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

II. POLICY

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

III. SCOPE

This policy governs the use of BWC's in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The chief or chief's designee may supersede this policy by providing specific instructions for BWC's use to individual officers, or providing specific instructions pertaining to particular events or classes of events, including but not limited to political rallies and demonstrations.

The chief or designee may also provide specific instructions or standard operating procedures for BWC's use to officers assigned to specialized details, such as carrying out duties in courts or guarding prisoners or patients in hospitals and mental health facilities

IV. DEFINITIONS

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

- I. MGDPA or Data Practices Act refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq.
- J. Records Retention Schedule refers to the General Records Retention Schedule for Minnesota Cities.
- K. Law enforcement-related information means information captured or available for capture by use of a BWC's that has evidentiary value because it documents events with respect to a stop, arrest, search, citation, or charging decision.
- L. 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.
- M. 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.
- N. Adversarial 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.
- O. Unintentionally recorded footage is a video recording that results from an officer's inadvertence or neglect in operating the officer's Portable Recording Device, 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.
- P. 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.

V. USE AND DOCUMENTATION

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

- G. Officers who have been issued BWC's shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWC's at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing
- H. Officers should wear their issued BWC's at the location on their body and in the manner specified in training.
- I. Officers must document BWC's use and non-use as follows:
 - 1. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report.
 - 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. Supervisors shall review these reports and initiate any corrective action deemed necessary.
- J. The department will maintain the following records and documents relating to BWC's use, which are classified as public data:
 - 1. The total number of BWC's owned or maintained by the agency;
 - 2. A daily record of the total number of BWC's actually deployed and used by officers and, if applicable, the precincts in which they were used;
 - 3. The total amount of recorded BWC's data collected and maintained; and
 - 4. This policy, together with the Records Retention Schedule.

VI. GENERAL GUIDELINES FOR RECORDING

- G. Officers shall activate their BWC's when responding to all calls for service and during all law enforcement-related encounters and activities, including but not limited to pursuits, *Terry* stops of motorists or pedestrians, arrests, searches, suspect interviews and interrogations, and during any police/citizen contacts that becomes 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 documented as specified in the Use and Documentation guidelines, part (D)(2) (above).
- H. Officers have discretion to record or not record general citizen contacts.
- I. Officers have no affirmative duty to inform people that a BWC's is being operated or that the individuals are being recorded.

- J. Once activated, the BWC's should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, officers shall state the reasons for ceasing the recording on camera before deactivating their BWC's. If circumstances change, officers shall reactivate their cameras as required by this policy to capture information having evidentiary value.
- K. Officers shall not intentionally block the Portable Recording Device's audio or visual recording functionality to defeat the purposes of this policy.
- L. Notwithstanding any other provision in this policy, officers shall not use their BWC's 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.

VII. SPECIAL GUIDELINES FOR RECORDING

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

- E. To use their BWC's 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.
- F. To use their BWC's 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.
- G. 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, BWC's shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.
- H. Officers shall use their Portable Recording Device 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.

VIII. DOWNLOADING AND LABELING DATA

- E. Each officer using a BWC's is responsible for transferring or assuring the proper transfer of the data from his or her camera to upload to the Watchguard/Motorola system 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 or investigator shall take custody of the officer's Portable Recording Device and assume responsibility for transferring the data from it.

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

15. Accidental Record
16. Citizen Contact
17. Traffic - Citation
18. Traffic - Warning
19. Fleeing in Motor Vehicle
20. Traffic Inv./Other
21. Motorist Assist
22. Suspicious Vehicle/Behavior
23. Test Recording
24. Narcotics Investigation
25. Investigation/Other
26. Assault
27. Medical
28. SRO/School

- G. In addition, officers shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under the MGDPA limiting disclosure of information about them. These individuals include:

15. Victims and alleged victims of criminal sexual conduct and sex trafficking.
16. Victims of child abuse or neglect.
17. Vulnerable adults who are victims of maltreatment.
18. Undercover officers.
19. Informants.
20. When the video is clearly offensive to common sensitivities.
21. Victims of and witnesses to crimes, if the victim or witness has requested not to be identified publicly.
22. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system.
23. Mandated reporters.

24. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness.
 25. Juveniles who are or may be delinquent or engaged in criminal acts.
 26. Individuals who make complaints about violations with respect to the use of real property.
 27. Officers and employees who are the subject of a complaint related to the events captured on video.
 28. Other individuals whose identities the officer believes may be legally protected from public disclosure.
- H. Labeling and flagging designations may be corrected or amended based on additional information.

IX. ADMINISTERING ACCESS TO BWC'S DATA

- H. Data subjects. Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC's data:
4. Any person or entity whose image or voice is documented in the data.
 5. The officer who collected the data.
 6. 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
- I. BWC's data is presumptively private. BWC's recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:
4. BWC's data pertaining to people is presumed private, as is BWC's data pertaining to businesses or other entities.
 5. Some BWC's data is classified as confidential (see C. below).
 6. Some BWC's data is classified as public (see D. below).
- J. Confidential data. BWC's 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.
- K. Public data. The following BWC's data is public:
5. 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.
 6. Data that documents the use of force by a peace officer that results in substantial bodily harm.

7. 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.
 8. 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.
- L. Access to BWC's data by non-employees. Officers shall refer members of the media or public seeking access to BWC's data to the Chief or designee, who shall process the request in accordance with the MGDPA and other governing laws. In particular:
3. An individual shall be **provided with access and allowed to review** recorded BWC's 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.
 4. 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.
- M. Access by peace officers and law enforcement employees. No employee may have access to the department's BWC's data except for legitimate law enforcement or data administration purposes:
4. Officers may access and view stored BWC's video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Except as provided in the critical incident response policy, 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.

5. Agency personnel shall document their reasons for accessing stored BWC's data in the manner provided within the database at the time of each access. Agency personnel are prohibited from accessing BWC's data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC's data recorded or maintained by this agency to public and social media websites.
 6. Employees seeking access to BWC's data for non-business reasons may make a request for it in the same manner as any member of the public.
- N. Other authorized disclosures of data. Officers may display portions of BWC's 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 screen shots, muting the audio, or playing the audio but not displaying video. In addition,
1. BWC's 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's data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

X. DATA SECURITY SAFEGUARDS

- B. The data security safeguards will be handled by the IT personnel contracted by the City of Hawley Police Department.
- E. Access to BWC's data from city or personally owned and approved devices shall be managed in accordance with established city policy.
- F. Officers shall not intentionally edit, alter, or erase any BWC's recording unless otherwise expressly authorized by the chief or the chief's designee.
- G. 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's program.

XI. AGENCY USE OF DATA

- E. At least once a month, supervisors will randomly review BWC's usage by each officer to whom a BWC's is issued or available for use, to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.
- F. In addition, supervisors and other assigned personnel may access BWC's 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.
- G. Nothing in this policy limits or prohibits the use of BWC's data as evidence of misconduct or as a basis for discipline.
- H. Officers should contact their supervisors to discuss retaining and using BWC's footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training officers may utilize BWC's data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

XII. DATA RETENTION

- I. All BWC's data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.
- J. 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.
- K. Certain kinds of BWC's data must be retained for six years:
 - 3. 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.
 - 4. Data documenting circumstances that have given rise to a formal complaint against an officer.
- L. 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.
- M. Subject to Part F (below), all other BWC's footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.
- N. Upon written request by a BWC's 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.
- O. The department shall maintain an inventory of BWC's recordings having evidentiary value.

- P. The department will post this policy, and the following retention rules on the City of Hawley's website <https://hawley.govoffice.com/police>

I. Retention Rules

17. Default	90 days
18. Accidental Record	90 days
19. Citizen Contact	1095 days (3 years)
20. Traffic Citation	1095 days (3 years)
21. Traffic Warning	90 days
22. Fleeing in MV	2555 days (7 years)
23. DWI/DUI	2555 days (7 years)
24. Traffic Inv/Other	2555 days (7 years)
25. Motorist Assist	90 days
26. Suspicious Vehicle/Behavior	90 days
27. Test Recording	90 days
28. Narcotics Investigation	2555 days (7 years)
29. Investigation (Other)	2555 days (7 years)
30. Assault	2555 days (7 years)
31. Medical	90 days
32. SRO/School	90 days

XIII. COMPLIANCE

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

