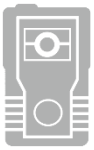
INDEPENDENT AUDITOR'S REPORT

University of Minnesota Police Department



DECEMBER 4TH, 2024

RAMPART AUDIT LLC

Audit Overview and Recommendations

Dear University of Minnesota Board of Regents and Chief Clark:

We have audited the body-worn camera (BWC) program of the University of Minnesota Police Department (UMPD) for the two-year period ended 8/24/2023. 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 University of Minnesota Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On September 27, 2024, Rampart Audit LLC (Rampart) met with Records Administrator Chelsea Gustafson, who provided information about UMPD'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 UMPD's recordkeeping.

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

UMPD 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.

The University of Minnesota Police Department serves the Twin Cities, Duluth and Morris campuses of the University of Minnesota system. The Crookston and Rochester campuses do not have University police departments. UMPD's BWC program began operation on August 25, 2021. UMPD personnel provided documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the implementation of UMPD's BWC program. Specifically, UMPD personnel furnished the following as evidence that UMPD had met these requirements:

1. A document titled "Board of Regents Public Comment Period," describing a public comment hearing to be held on March 12, 2021, and providing internet links for interested parties to either sign up speak during the hearing, or to submit written comments in advance.
2. A copy of the March 12, 2021, University of Minnesota Board of Regents meeting agenda listing the BWC public hearing as the first item on the agenda.

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

3. A copy of the March 12, 2021, University of Minnesota Board of Regents meeting minutes documenting the BWC public hearing.
4. A link to a video recording of the public hearing, which was held via videoconference, that is publicly available on YouTube.

Copies of these documents have been retained in Rampart's audit files. In our opinion, the University of Minnesota 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."

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

UMPD BWC WRITTEN POLICY

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

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

1) The requirements of section 13.825 and other data classifications, access procedures, retention policies, and data safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;
2) A prohibition on altering, erasing or destroying any recording made with a peace officer's portable recording system or data and metadata related to the recording prior the expiration of the applicable retention period under section 13.825 Subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely;
3) A mandate that a portable recording system be worn at or above the mid-line of the waist in a position that maximizes the recording system's capacity to record video footage of the officer's activities;
4) A mandate that officers assigned a portable recording system wear and operate the system in compliance with the agency's policy adopted under this section while performing law enforcement activities under the command and control of another chief law enforcement officer or federal law enforcement official;
5) A mandate that, notwithstanding any law to the contrary, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency must allow the deceased individual's next of kin, the legal representative of the deceased individual's next of kin, and the other parent of the deceased individual's child, upon their request, to inspect all portable recording system data, redacted no more than what is required by law, documenting the incident within five days of the request, with the following exception:
    a) A law enforcement agency may deny a request if the agency determines that there is a compelling reason that inspection would interfere with an active investigation. If the agency denies access, the chief law enforcement officer must provide a prompt, written denial to the individual who requested the data with a short description of the compelling reason access was denied and must provide notice that relief may be sought from the district court pursuant to section 13.82 subdivision 7;
6) A mandate that, when an individual dies as a result of a use of force by a peace officer, an involved officer's law enforcement agency shall release all portable recording system data, redacted no more than required by law, documenting the incident no later than 14 days after the incident, unless the chief law enforcement officer asserts in

writing that the public classification would interfere with an ongoing investigation, in which case the data remain classified by section 13.82 subdivision 7;
7) Procedures for testing the portable recording system to ensure adequate functioning;
8) Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
9) Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
10) Circumstances under which a data subject must be given notice of a recording;
11) Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
12) Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
13) Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

In our opinion, the UMPD 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.

UMPD 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 UMPD's 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 one-year retention period for reportable firearms discharges.

The Data Retention section of the BWC policy specifies a six-year retention period for "[d]ata that documents [sic] 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," as well as "[d]ata documenting circumstances that have given rise to a formal complaint against an officer." We noted that this retention period exceeds the requirement for BWC data documenting a use of force by an officer that results in substantial bodily harm as well as data documenting an incident resulting in a formal complaint against an officer, but does not meet the "indefinite" retention requirement for BWC data that document an officer's use of deadly force.

UMPD's BWC policy contains the §13.825 Subd. 3(d) requirement pertaining to additional retention when so requested by a data subject.

The Data Security Safeguards section of UMPD's BWC policy states that: "[o]fficers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the Chief or authorized designee." We recommend amending this section to clarify that under no circumstances may any BWC data or metadata be altered, erased, or deleted prior to the expiration of the required retention period.

UMPD employs a mix of Axon Body 2 (AB2) and Body 3 (AB3) body-worn cameras and utilizes Axon's Evidence.com cloud-based storage service. UMPD uses the Axon Evidence video management software to manage BWC data retention through automated retention settings. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be manually adjusted as needed. If an officer fails to assign a data classification, the default retention period is 90 days.

In our opinion, UMPD's written BWC policy is compliant with respect to applicable data retention requirements, with the exception of the following:

1. Recordings of incidents documenting the use of deadly force must be retained indefinitely;
2. A written policy must explicitly prohibit the alteration, erasure or destruction of any BWC recording prior to the expiration of its retention date.

Prior to the issuance of this report, UMPD submitted a revised BWC policy that addresses the exceptions noted above. In our opinion, this revised BWC policy is compliant with respect to the applicable data retention requirements. A copy of this policy has been attached to this report as Appendix B.

UMPD BWC Data Destruction

As discussed above, UMPD utilizes Axon's Evidence.com for storage, with retention periods determined based on the classification assigned to BWC data. Axon certifies that its Cloud Service is compliant with the Federal Bureau of Investigation's Criminal Justice Information System Security Division Policy as required by Minnesota Statute §13.825 Subd. 11(b). Data destruction is achieved through automated deletion and overwriting, with storage devices sanitized (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, UMPD's written BWC policy is compliant with respect to the applicable data destruction requirements.

UMPD BWC Data Access

UMPD's BWC policy states that the BWC Program Coordinator is responsible for processing requests from members of the public or the media for access to BWC data. All such requests are made online through the University of Minnesota Data Request Center (umn.nextrequest.com), and are processed "in accordance with University of Minnesota policies and other governing laws." UMPD evidence personnel process the requests and perform any necessary redaction. Data subjects receive BWC data via email.

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. At the time of our audit, UMPD had not revised its BWC policy to address these requirements.

UMPD's BWC policy also states that BWC data "may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure." UMPD maintains a copy of each such request it receives. In addition, BWC data "shall be made available to prosecutors, courts, and other criminal justice entities as provided by law." Requests for BWC data from outside agencies and prosecutors may be made either through the Data Request Center or via email, and are fulfilled via an Evidence.com internet link.

Prior to releasing data, the receiving agency is given a verbal reminder of their obligations under §13.825 Subd. 7 and Subd. 8, which include a requirement to maintain BWC data security. The University of Minnesota Police Department noted and put in their policy that they will be adding a written reminder or an email of the receiving agency's obligations each time a data request is fulfilled.

In our opinion, UMPD's written BWC policy is compliant with respect to the applicable data access requirements, with the following exceptions:

1. The BWC policy must state 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, unless 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.
2. The BWC policy must state 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.
3. While UMPD's 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," they did not provide any information about steps taken to ensure the receiving agency will comply with §13.825 Subd. 8(b).

Prior to the issuance of this report, UMPD submitted a revised BWC policy that addresses the exceptions noted above. In our opinion, this revised BWC policy is compliant with respect to the applicable data access requirements.

UMPD BWC Data Classification

UMPD's BWC Policy states that "BWC data is presumptively private," and further states that "BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently." Active criminal

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

As noted in the preceding section, prior to the issuance of this report, University of Minnesota Police Department furnished a revised BWC policy to address the 2023 legislative updates regarding data documenting incidents involving the use of deadly force. The revisions quote directly from the updated statute. This section of the UMPD 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.

UMPD BWC Internal Compliance Verification

The UMPD BWC Training and Compliance section states that "[s]upervisors shall monitor for compliance with this policy," while the Agency Use of Data section states that "[a]t least once a month, supervisors will randomly review BWC usage by each officer to whom a BWC is issued or available for use, to ensure compliance with this policy."

The Axon Evidence software logs all video access, including supervisory reviews.

UMPD's BWC policy states that:

> Officers may only use 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 who have been issued BWCs shall operate and use them consistent with this policy.

The 2023 legislative changes require that an agency's BWC policy must specify that an officer assigned a BWC must 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. While the wording in UMPD's BWC policy appears to be sufficiently broad to cover such scenarios, we recommend adding language to make this requirement explicit.

Prior to the issuance of this report, UMPD submitted a revised version of their BWC policy adding the language described in the preceding paragraph. A copy of the revised policy is attached to this report as Appendix B.

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

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

UMPD BWC Program and Inventory

UMPD currently possesses 107 Axon body-worn cameras, which include Body 2 and Body 3 models.

The UMPD BWC policy identifies those circumstances in which deputies 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. For Patrol personnel, the Panasonic body-worn cameras are synced to their squad camera systems and are activated automatically anytime the squad's emergency lights are activated.

UMPD's BWC policy states that "[o]fficers should wear their issued BWCs at the location on their body and in the manner specified in training." The 2023 legislative changes specify that a BWC policy must require that a BWC "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."

Prior to the issuance of this report, UMPD submitted a revised version of their BWC policy clarifying that "Officers should wear their issued BWCs at the location on their body 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, and in the manner specified in training."

UMPD administrators are able to determine the number of BWCs deployed by reviewing the schedule and/or payroll data.

As of the audit date, September 27, 2024, UMPD maintained 47,411 BWC events, totaling approximately 25,477.89 GB of data.

UMPD BWC Physical, Technological and Procedural Safeguards

UMPD BWC data are initially recorded to a hard drive in each officer's BWC. Prior to the end of each shift, the officer places his or her BWC in a docking station at their UMPD facility. Any BWC data are then uploaded automatically to Axon's cloud service.

Officers have view access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes. Only administrators have the ability to delete recordings. All BWC data access is logged automatically and available for audit purposes, and officers are required to provide a reason each time a video is accessed.

Enhanced Surveillance Technology

UMPD 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 UMPD 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

Because UMPD was unable to provide a list of calls for service prior to the audit, Rampart utilized an alternate method to select a random sample of 132 date/time combinations 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 UMPD records.

Audit Conclusions

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

Daniel E. Gazelka

Daniel E. Gazelka

Rampart Audit LLC

12/04/2024

APPENDIX A:

Policy

446

University of Minnesota Police Department

University of Minnesota PD Policy Manual (Issued on 05-09-2023)

Body Worn Cameras

446.1 PURPOSE

The primary purpose of using body-worn-cameras (BWCs) is to capture evidence arising from police- citizen encounters by members of the University of Minnesota Police Departments (Duluth, Morris, and Twin Cities) (each referenced in this policy individually as "Department"). 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.

446.2 POLICY

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

446.3 SCOPE

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad- based (dash-cam) recording systems. The Chief of Police or authorized designee may supersede this policy by providing specific instructions for BWC use to individual officers, or providing specific instructions pertaining to particular events or classes of events, including but not limited to political rallies, demonstrations, ceremonial events, and department gatherings. The Chief or authorized designee may also provide specific instructions or standard operating procedures for BWC 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.

446.4 DEFINITIONS

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

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

Records Retention Schedule refers to the University of Minnesota's Record Retention Schedule.

Law enforcement-related information means information captured or available for capture by

use of a BWC that has evidentiary value because it documents events with respect to a stop, arrest, search, citation, or charging decision.

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.

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.

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

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.

446.5USE AND DOCUMENTATION

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

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

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

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

1. Whenever an officer makes a recording, the existence of the recording shall be documented in a CAD record.

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 a CAD record. Supervisors shall be notified by the officer, review the report and initiate any corrective action deemed necessary.

E. The Department's BWC Program Coordinator will maintain the following records and documents relating to BWC use, which are classified as public data:

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

2. A daily record of the total number of BWCs actually deployed and used by officers and, if applicable, the precincts in which they were used;
3. The total amount of recorded BWC data collected and maintained; and
4. This policy, together with the Records Retention Schedule.

446.6 GENERAL GUIDELINES FOR RECORDING

A. Officers shall activate their BWCs 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, during any police/citizen contacts that become adversarial, and if directed by a supervisor. 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 is being operated or that the individuals are being recorded.

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

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

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

446.7 SPECIAL GUIDELINES FOR RECORDING

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

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

B. To use their BWCs 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.

In addition,

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, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.

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

E. Officers need not record interactions with undercover officers or confidential informants.

F. Officers should use caution using BWCs where an explosive device may be present or during protective sweeps for explosive devices.

446.8 DOWNLOADING AND LABELING DATA

A. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from the officer's camera 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 BWC and assume responsibility for transferring the data from it.

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

1. **Evidence—criminal:** The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision.

2. **Evidence—force:** Whether or not enforcement action was taken, or an arrest resulted, the event involved the application of force by an officer of this agency of sufficient degree or under circumstances triggering a requirement for supervisory review.

3. **Evidence—property:** Whether or not enforcement action was taken, or an arrest resulted, an officer seized property from an individual or directed an individual to dispossess property.

4. **Evidence—administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer.

5. **Evidence—other:** The recording has potential evidentiary value for reasons identified by the officer at the time of labeling.

6. **Training:** The event was such that it may have value for training.

7. **Not evidence:** The recording does not contain any of the foregoing categories of information and has no apparent evidentiary value. Recordings of general citizen contacts and unintentionally recorded footage are not evidence.

C. In addition, officers shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under related law or policy 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.

446.9 ADMINISTERING ACCESS TO BWC DATA

A. **Data subjects.** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:

1. Any person or entity whose image or voice is documented in the data.
2. The officer who collected the data.
3. Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.

B. **BWC data is presumptively private.** BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:

1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.
2. Some BWC data is classified as confidential (see C. below).
3. Some BWC data is classified as public (see D. below).

C. **Confidential data.** BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above and the "public" classifications listed below.

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

1. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.
2. Data that documents the use of force by a peace officer that results in substantial bodily harm.
3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted if practicable. In addition, any data on undercover officers must be redacted.
4. Data that documents the final disposition of a disciplinary action against a public employee.

However, if another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other classification. For instance, data that reveals protected identities under Minn. Stat. § 13.82, subd. 17 (e.g., certain victims, witnesses, and others) should not be released even if it would otherwise fit into one of the public categories listed above.

E. **Access to BWC data by non-employees.** Officers shall refer members of the media or public seeking access to BWC data to the Department's BWC Program Coordinator who shall process the requesting accordance with University of Minnesota policies and other governing laws. In particular:

1. An individual shall be provided with access and allowed to review recorded BWC data about that individual 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.

3. If a person brings an action in district court under MN Statute section 13.825 subd. 2, the Department shall give notice to any data subjects in the video in question who did not receive notice from the person bringing the action, if known.

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

1. Officers may access and view stored BWC video 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.

2. Agency personnel shall document their reasons for accessing stored BWC data within the BWC database 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.

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

G. **Other authorized disclosures of data.** Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of 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 data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure.

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

446.10 DATA SECURITY SAFEGUARDS

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

B. Access to BWC data from DPS or personally-owned and approved devices shall be managed in accordance with established UMN policy.

C. Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the Chief or authorized designee.

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

446.11 AGENCY USE OF DATA

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

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

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

D. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. 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 data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

446.12 DATA RETENTION

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

B. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.

C. Certain kinds of BWC 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 footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.

F. Upon written request by a BWC data subject, the DPS shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. DPS 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. DPS shall maintain an inventory of BWC recordings having evidentiary value.

H. DPS will post this policy on its website.

446.13 COMPLIANCE

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

APPENDIX B:

Policy

446

University of Minnesota Police Department

University of Minnesota PD Policy Manual (Issued on 05-09-2023)

Body Worn Cameras

446.1 PURPOSE

The primary purpose of using body-worn-cameras (BWCs) is to capture evidence arising from police-citizen encounters by members of the University of Minnesota Police Departments (Duluth, Morris, and Twin Cities) (each referenced in this policy individually as "Department"). 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.

446.2 POLICY

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

446.3 SCOPE

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The Chief of Police or authorized designee may supersede this policy by providing specific instructions for BWC use to individual officers, or providing specific instructions pertaining to particular events or classes of events, including but not limited to political rallies, demonstrations, ceremonial events, and department gatherings. The Chief or authorized designee may also provide specific instructions or standard operating procedures for BWC 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.

446.4 DEFINITIONS

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

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

Records Retention Schedule refers to the University of Minnesota's Record Retention Schedule.

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

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.

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.

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

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.

446.5 USE AND DOCUMENTATION

A. Officers may use only Department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this Department. Officers shall follow this policy even when acting under the command and control of a chief law enforcement from another agency or a federal law enforcement official.

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

C. Officers should wear their issued BWCs at the location on their body 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, and in the manner specified in training.

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

1. Whenever an officer makes a recording, the existence of the recording shall be documented in a CAD record.

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 a CAD record. Supervisors shall be notified by the officer, review the report and initiate any corrective action deemed necessary.

E. The Department's BWC Program Coordinator will maintain the following records and documents relating to BWC use, which are classified as public data:

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

2.A daily record of the total number of BWCs actually deployed and used by officers and, if applicable, the precincts in which they were used;

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

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

446.6 GENERAL GUIDELINES FOR RECORDING

A. Officers shall activate their BWCs 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, during any police/citizen contacts that become adversarial, and if directed by a supervisor. 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 is being operated or that the individuals are being recorded.

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

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

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

446.7 SPECIAL GUIDELINES FOR RECORDING

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

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

B. To use their BWCs 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.

In addition,

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, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.

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

E. Officers need not record interactions with undercover officers or confidential informants.

F. Officers should use caution using BWCs where an explosive device may be present or during protective sweeps for explosive devices.

446.8 DOWNLOADING AND LABELING DATA

A. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from the officer's camera 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 BWC and assume responsibility for transferring the data from it.

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

1. **Evidence—criminal:** The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision.

2. **Evidence—force:** Whether or not enforcement action was taken, or an arrest resulted, the event involved the application of force by an officer of this agency of sufficient degree or under circumstances triggering a requirement for supervisory review.

3. **Evidence—property:** Whether or not enforcement action was taken, or an arrest resulted, an officer seized property from an individual or directed an individual to dispossess property.

4. **Evidence—administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer.

5. **Evidence—other:** The recording has potential evidentiary value for reasons identified by the officer at the time of labeling.

6. **Training:** The event was such that it may have value for training.

7. **Not evidence:** The recording does not contain any of the foregoing categories of information and has no apparent evidentiary value. Recordings of general citizen contacts and unintentionally recorded footage are not evidence.

C. In addition, officers shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under related law or policy 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.

B. Labeling and flagging designations may be corrected or amended based on additional information.

446.9 ADMINISTERING ACCESS TO BWC DATA

A. **Data subjects.** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:

1. Any person or entity whose image or voice is documented in the data.

2. The officer who collected the data.

3. Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.

B. BWC data is presumptively private. BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:

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

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

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

B. **Confidential data.** BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the “private” classification listed above and the “public” classifications listed below.

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

1. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.

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

3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted if practicable. In addition, any data on undercover officers must be redacted.

4. Data that documents the final disposition of a disciplinary action against a public employee.

However, if another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other classification. For instance, data that reveals protected identities under Minn. Stat. § 13.82, subd. 17 (e.g., certain victims, witnesses, and others) should not be released even if it would otherwise fit into one of the public categories listed above.

E. Access to BWC data by non-employees. Officers shall refer members of the media or public seeking access to BWC data to the Department's BWC Program Coordinator who shall process the requesting accordance with University of Minnesota policies and other governing laws. In particular:

1. An individual shall be provided with access and allowed to review recorded BWC data about that individual 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.

1. If a person brings an action in district court under MN Statute section 13.825 subd. 2, the Department shall give notice to any data subjects in the video in question who did not receive notice from the person bringing the action, if known.

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

1. Officers may access and view stored BWC video 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.

2. Agency personnel shall document their reasons for accessing stored BWC data within the BWC database 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.

3. 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.

C. **Deadly Force Data.** Data documenting a law enforcement encounter involving deadly force is required to be released with no more redaction than is required by law under the following conditions:

1. Within 5 days of the request to the deceased individual's next of kin, the legal representative of the deceased's next of kin, and the other parent of the deceased individual's child.

2. Within 14 days of the incident occurrence.

Requests for this data may be denied if a compelling reason exists that indicates release would interfere with an active investigation. This must be asserted in writing in accordance with Minn. Stat. 13.825 Subd. 2.

H. Other authorized disclosures of data. Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individual identities that are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition:

1. BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure. In accordance with MN Statute 13.825 Subd. 8(b), requesting agencies shall be informed by email or in writing to treat any video received as if it were their own.

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

446.10 DATA SECURITY SAFEGUARDS

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

B. Access to BWC data from DPS or personally-owned and approved devices shall be managed in accordance with established UMN policy.

C. Officers shall not intentionally edit, alter, or erase any BWC recording, data, or metadata unless otherwise expressly authorized by the Chief or authorized designee, and in no case prior to the expiration of the applicable retention period under section 13.825 subdivision 3, except that the full, unedited, and unredacted recording of a peace officer using deadly force must be maintained indefinitely.

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

446.11 AGENCY USE OF DATA

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

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

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

D. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. 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 data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

446.12 DATA RETENTION

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

B. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.

C. Certain kinds of BWC 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 footage that is classified as non-evidentiary,

becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.

F. Upon written request by a BWC data subject, the DPS shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. DPS 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. DPS shall maintain an inventory of BWC recordings having evidentiary value.

H. DPS will post this policy on its website.

446.13 COMPLIANCE

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