



# INDEPENDENT AUDITOR'S REPORT

---

Starbuck Police Department



AUGUST 29TH, 2023  
RAMPART DEFENSE LLC  
P.O. Box 23 Clearbrook, MN 56634

## **Audit Overview and Recommendations**

Dear Starbuck City Council and Chief Johnsrud:

We have audited the body-worn camera (BWC) program of the Starbuck Police Department (SPD) for the two-year period ended 5/31/2023. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)<sup>1</sup> program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Starbuck Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On July 31, 2023, Rampart Defense LLC (Rampart) met with Administrative Assistant Charleen Drewes, who provided information about SPD'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 SPD's recordkeeping.

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

### **SPD BWC Program Implementation and Authorization**

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

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

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

Rampart previously audited SPD's BWC program in 2021. During that audit, Chief Mitch Johnsrud advised us that while SPD had employed body-worn cameras since approximately 2006, the agency

---

<sup>1</sup> 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 SPD, these terms may be used interchangeably in this report.

suspended their use from August 1, 2016, until March 13, 2017, while the BWC policy and program were updated to comply with Minnesota Statute §626.8473.

Chief Johnsrud provided documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the re-implementation of SPD's BWC program. Specifically, Chief Johnsrud furnished a copy of the City of Starbuck "Minutes of Public Hearing on Body Worn Camera Policy," dated March 13, 2017, as well as a copy of the City of Starbuck "Minutes of Regular City Council Meeting," also dated March 13, 2017. Copies of these documents have been retained in Rampart's audit files. In our opinion, Starbuck Police Department met the public notice and comment requirements prior to the reimplementation of their BWC program.

As part of the current audit, Chief Johnsrud provided a copy of SPD's written BWC policy and a link to this policy on SPD's page on the City of Starbuck website. Rampart staff then verified that this was a working link. In our opinion, Starbuck Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

### **SPD BWC WRITTEN POLICY**

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

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

1. The requirements of section 13.825 and other data classifications, access procedures, retention policies, and data safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;
2. Procedures for testing the portable recording system to ensure adequate functioning;
3. Procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure;
4. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
5. Circumstances under which a data subject must be given notice of a recording;
6. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
7. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
8. Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

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

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

### **SPD BWC Data Retention**

SPD's data retention policy states that "[a]ll BWC data shall be retained for a minimum period 90 days. There are no exceptions for erroneously recorded or non-evidentiary data." This is compliant with the statutory requirement that all BWC data be maintained for at least 90 days.

§13.825 Subd. 3(b) requires that the following categories of BWC data be retained for a minimum of one year:

1. Data documenting the discharge of a firearm by a peace officer in the course of duty if a notice is required under §626.533 Subd. 2;
2. Data documenting use of force by the officer resulting in substantial bodily harm; or
3. A formal complaint is made against a peace officer related to the incident.

SPD's data retention guidelines meet or exceed the requirements specified for each category of BWC data listed above. Specifically, the SPD policy lists a retention period of one year for data in the first category and six years for data in the second or third categories.

§13.825 Subd. 3(c) requires that the agency retain BWC data for an additional time period of up to 180 days if so requested in writing by a data subject. SPD's policy addresses this in language that quotes from the statute.

SPD's policy further notes that "[o]ther 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."

SPD employs Getac body-worn cameras and manages BWC data retention through that vendor's proprietary software, which is set to automatically overwrite videos at 90 days, unless a longer retention period has been specified.

SPD's BWC policy requires that each officer transfer data from his or her body-worn camera to the appropriate server by the end of each shift, and also requires that the officer assign the appropriate label or labels to each file to identify the nature of the data. These labels then determine the appropriate retention period for each file.

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

### **SPD BWC Data Destruction**

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

Getac 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.

SPD previously employed Watchguard body-worn cameras. While those cameras are no longer in use, SPD continues to contract with Watchguard's cloud service to store those BWC recordings for which the retention period has yet to expire.

As is the case with Getac, Watchguard also utilizes Microsoft's Azure Government environment for its cloud storage service, and the same compliance certifications discussed above also apply.

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

### **SPD BWC Data Access**

Any requests for access to BWC data by data subjects would be facilitated by Chief Johnsrud in accordance with the provisions of §13.825 Subd. 4(b).

SPD BWC data is shared with other law enforcement agencies for evidentiary purposes only. All such requests must be made to Chief Johnsrud by the requesting agency's chief law enforcement officer (CLEO). Existing verbal agreements between SPD and other area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b).

Access to SPD BWC data for outside agencies is provided via an e-mailed weblink. These links most commonly permit either one-time access, or access for up to 90 days before expiring. Links provided to the Pope County Attorney's Office normally permit access for up to 180 days.

All requests are documented in the emails containing the weblinks. These requests are attached to the ICR and retained indefinitely. In addition, the Watchguard software creates a log of all weblinks created to provide access to SPD BWC data. This log can be audited at any time.

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

### **SPD BWC Data Classification**

SPD follows the BWC data classifications set forth in Minnesota Statute §13.825, and the written BWC policy incorporates the statutory language extensively. Specifically, SPD identifies BWC data as presumptively private, while also identifying those exceptions under which such data are classified as either confidential or public. The policy further notes that other provisions of the Data Practices Act may supersede the public classification. In our opinion, this section of the policy is compliant with respect to the applicable data classification requirements.

### **SPD BWC Internal Compliance Verification**

The SPD BWC Agency Use of Data section states that:

At least once a month, supervisors will randomly review BWC usage by each officer to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is necessary.

In addition, the SPD BWC Compliance section states that:

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

During the 2021 audit, Chief Johnsrud advised Rampart that the SPD personnel policy addresses specific actions and consequences in greater detail. Rampart confirmed during the current audit that these practices have not changed.

In our opinion, these provisions meet the requirements of §626.8473 Subd. 3(b)(8) regarding procedures to ensure compliance and address violations of the written BWC policy.

### **SPD BWC Program and Inventory**

SPD currently possesses four (4) Getac body-worn cameras.

The SPD 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.

While SPD does not maintain a separate log of BWC deployment or use, because each patrol officer wears a BWC while on duty, the number of BWC units deployed each shift can be determined based on a review of SPD payroll records. BWC use would be determined based on the creation of BWC data.

As of 7/31/2023, SPD maintained 1,334 files of BWC data.

### **SPD BWC Physical, Technological and Procedural Safeguards**

SPD BWC data are initially recorded to a hard drive in each officer's body-worn camera. Those files are then transferred through an automated process to Getac's cloud service utilizing a cellular connection. In the event the automated upload process fails, data can also be transferred through the use of a physical docking station at the Starbuck Police Department.

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

As noted above, requests by other law enforcement agencies for SPD BWC data must be approved by Chief Johnsrud and are fulfilled through an expiring weblink submitted to the requesting agency or officer via email. A similar method is employed to submit SPD BWC data to the Pope County Attorney's Office.

### **Enhanced Surveillance Technology**

SPD 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 SPD 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 CFSs 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 ICRs 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 SPD records.

### **Audit Conclusions**

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



Daniel E. Gazelka

Rampart Defense LLC

8/29/2023

# APPENDIX A:

SECTION 8 – BODY WORN CAMERA GENERAL ORDER 47 BODY WORN CAMERA POLICY (Updated 6/9/2021) PURPOSE The primary purpose of using body-worn-cameras (BWCs) is to capture evidence arising from police-citizen encounters. This policy sets forth guidelines governing the use of BWCs and administering the data that results. Compliance with these guidelines is mandatory, but it is recognized that officers must also attend to other primary duties and the safety of all concerned, sometimes in circumstances that are tense, uncertain, and rapidly evolving. 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. 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 or chief’s designee may supersede this policy by providing specific instructions for BWC use to individual officers or providing specific instructions pertaining to 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 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. 47.1 DEFINITIONS The following phrases 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 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 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. 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. 47.2 USE AND DOCUMENTATION A. Officers may use only department issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this department. B. Officers who



have been issued BWCs shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing. C. Officers 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 an incident report or on the Evidence Section in RMS (LETG) if no report is written. 2. Whenever an officer fails to record an activity that is required to be recorded under this policy or captures only a part of the activity, the officer must document the circumstances and reasons for not recording in an incident report or in the Case Notes in RMS (LETG) if no report is written. 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 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 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.

#### 47.3 GENERAL GUIDELINES FOR RECORDING

A. Officers shall activate their BWCs when anticipating that they will be involved in, become involved in, or witness other officers of this agency involved in a pursuit, Terry stops a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value. 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 postshift time in locker rooms, during meal breaks, or during other private conversations, unless recording is authorized as part of an administrative or criminal investigation.

#### 47.4 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 and 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.

47.5 DOWNLOADING AND LABELING DATA A. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera to that officer's folder located on the digital evidence computer 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 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. Evidence—criminal: The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision.
2. Evidence—force: Whether enforcement action was taken, or an arrest resulted, the event involved the application of force by a law enforcement officer of this or another agency.
3. Evidence—property: Whether 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 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.

47.6 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 Chief of Police/Administrative Assistant who shall process the request in accordance with the MGDPA and other governing laws. In particular: 1. An individual shall be allowed to review recorded BWC data about him- or herself and other data subjects in the recording, but access shall not be granted: a. If the data was collected or created as part of an active investigation. b. To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17. 2. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction: a. Data on other individuals in the recording who do not consent to the release must be redacted. b. Data that would identify undercover officers must be redacted. c. Data on other officers who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted. 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. 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 data within incident reports/supplements/case notes to the case file relate to the video, 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 individuals whose identities 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. 47.7 DATA SECURITY SAFEGUARDS A. All BWC files recorded will be uploaded through GETAC software to the cloud to prevent any data loss. B. 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. C. Officers shall not intentionally edit, alter, or erase any BWC 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 program. 47.8 AGENCY USE OF DATA A. At least once a month, supervisors will randomly review BWC usage by each officer 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 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. 47.9 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 agency shall retain a recording pertaining to that subject for an additional time requested by the subject of up to 180 days. The agency will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received. G. The department shall maintain an inventory of BWC recordings having evidentiary value. H. The department will post this policy, together with its Records Retention Schedule, on its website. 47.10 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. FOR ANY OTHER OFFICER MISCONDUCT INVESTIGATIONS PLEASE REFER TO SECTION 2 (CONDUCT AND DISCIPLINE) IN GENERAL ORDERS 7 THROUGH 12 IN THIS POLICY MANUAL. – UPDATED 6-29-2021