INDEPENDENT AUDITOR'S REPORT

Sherburne County Sheriff's Office Body-Worn Camera Program

NOVEMBER 18, 2022

RAMPART DEFENSE LLC
P.O. Box 23 Clearbrook, MN 56634

Audit Overview and Recommendations

Dear Sherburne County Board and Sheriff Brott:

We have audited the body-worn camera (BWC) program of the Sherburne County Sheriff's Office (SCSO) for the two-year period ended 7/31/2022. 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 Sherburne County Sheriff's Office. Our responsibility is to express an opinion on the operations of this program based on our audit.

On September 13, 2022, Rampart Defense LLC (Rampart) met with Chief Deputy Steve Doran, who provided information about SCSO'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 SCSO's recordkeeping.

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

SCSO 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."

Chief Deputy Doran provided documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the implementation of SCSO's BWC program on August 31, 2018. Specifically, Chief Deputy Doran furnished a copy of the minutes of the May 1, 2018, Sherburne County Board meeting, which noted that a public hearing would be held on May 22, 2018, for the purpose of considering SCSO's new body-worn camera policy. Chief Deputy Doran also furnished a

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

copy of the minutes for the May 22, 2018, Sherburne County Board meeting, which noted that a public hearing was opened for the purpose of obtaining public input and addressing any questions, issues, concerns or other items related to SCSO's proposed BWC policy. Copies of these documents have been retained in Rampart's audit files. Rampart staff also verified that there was a working link to the Sherburne County Sheriff's Office's written BWC policy on their webpage at the time of our audit.

SCSO BWC WRITTEN POLICY

As part of this audit, we reviewed SCSO'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 SCSO BWC policy is compliant with respect to clauses 2 – 6.

SCSO BWC Data Retention

The data retention section of SCSO's BWC policy states that "BWC data shall be maintained for a minimum period of 90 days." The policy also itemizes the individual data categories identified in §13.825 Subd. 3 and provides the same retention period specified in statute for each. With respect to BWC data having evidentiary value, SCSO follows the General Records Retention Schedule for Minnesota Counties. Finally, the policy specifies that when a video meets multiple categories, it will be retained for the longest applicable retention period.

SCSO employs WatchGuard Vista body-worn cameras and manages BWC data retention on their own secure servers through automated retention settings in the video management software. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be adjusted as needed.

SCSO's BWC policy requires that each deputy transfer data from his or her body-worn camera to the appropriate server by the end of each shift, and also requires that the deputy 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, SCSO's written BWC policy is compliant with respect to applicable data retention requirements.

SCSO BWC Data Destruction

Chief Deputy Doran advised us that SCSO BWC data are stored on two servers located on-site, with one server dedicated to BWC data generated by non-sworn corrections workers employed at the Sherburne County Jail and the other server dedicated to BWC data generated by sworn deputies. The "jail" server utilizes a SAN RAID system, while the "deputy" server is backed up to an Exagrid disk system and, ultimately, to magnetic tape.

Data on the existing server are destroyed through automated deletion and overwriting, based on a retention schedule assigned to each video. In addition, at the time it is retired from service, any SCSO-owned physical hard drive used to store BWC data will have all data deleted prior to being destroyed by physical means, specifically crushing.

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

SCSO BWC Data Access

Any request for access to BWC data by data subjects would be made in writing to the SCSO Records Department. The records supervisor is then responsible for reviewing and fulfilling each request in accordance with the provisions of §13.825 Subd. 4(b).

SCSO BWC data is shared with other law enforcement agencies for evidentiary purposes only. All such requests must be made by email to the SCSO Records Department. Existing verbal agreements between SCSO and other area law enforcement agencies address data classification, destruction and security requirements, as specified in §13.825 Subd. 8(b). At the time of the audit, SCSO was in the process of preparing a written form to document acknowledgment of these requirements from requesting agencies. Access to SCSO BWC data for outside agencies is provided via optical disc.

We recommend that SCSO obtain a written acknowledgement from any outside law enforcement agency that any BWC data obtained from SCSO will be managed by the requesting agency in compliance with the requirements of §13.825 Subd. 7 and 8. A copy of this written acknowledgment should be maintained on file.

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

SCSO BWC Data Classification

SCSO follows the BWC data classifications set forth in Minnesota Statute §13.825, and the written BWC policy incorporates the statutory language extensively. In our opinion, this section of the policy is compliant with respect to the applicable data classification requirements.

SCSO BWC Internal Compliance Verification

The Compliance section of the SCSO BWC policy states that "[s]upervisors 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." Chief Deputy Doran advised us that each supervisor reviews a random selection of BWC videos for each of his or her direct reports every month to verify compliance. The Agency Use of Data section further notes that "[e]ach time a BWC video is reviewed within the WatchGuard [system], the employee shall note the reason why for auditing purposes."

In our opinion, these sections of the policy are compliant with the applicable internal compliance and disciplinary requirements.

SCSO BWC Program and Inventory

SCSO currently possesses 244 Watchguard body-worn cameras, deployed as follows:

- Patrol – 34
- ERU – 5
- SRO – 3
- Transportation/Court Security – 27
- Drug Task Force – 5
- Jail - 170

The SCSO 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.

The SCSO BWC policy states that "[d]eputies shall make sure their BWC is working properly at the beginning of each shift." Chief Deputy Doran advised that this is accomplished through the creation of a test recording. We recommend specifically including test recordings in the supervisory reviews discussed in the previous section as verification that BWCs are being tested at the start of each shift as required by policy.

While SCSO does not maintain a separate log of BWC deployment or use, Chief Deputy Doran advised us that because each uniformed deputy wears a BWC while on duty, the number of BWC units deployed with uniformed personnel each shift can be determined based on a review of SCSO payroll records. In addition, non-uniformed personnel are issued and authorized but not required to wear or use body-worn cameras. Actual BWC use would be determined based on the creation of BWC data.

As of the date of the audit, SCSO maintained 57.03 TB and 110.67 TB of BWC data on the respective servers.

SCSO BWC Physical, Technological and Procedural Safeguards

SCSO BWC data are initially recorded to an internal hard drive in each deputy's BWC. Those files are then transferred to a dedicated server at the SCSO office through a docking station connected to the server by a physical cable. The server is secured behind multiple locked doors.

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

As noted above, requests by other law enforcement agencies for SCSO BWC data must be submitted to the Records Department and are fulfilled via optical disc. A similar method is employed to submit SCSO BWC data to prosecutors.

While SCSO does employ systems to duplicate data from the two servers, it is our understanding that these duplicates are retained on-site. Though not required, we recommend the use of an off-site backup to guard against the loss of BWC data due not only to hardware failures associated with an individual server, but also due to physical hazards such as fires, floods or wind events. In our experience, many sheriff's offices utilize servers located at other county facilities, such as the highway department or county government offices, as an efficient and cost-effective means of establishing secure off-site storage.

Enhanced Surveillance Technology

SCSO 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 SCSO 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.

Jail

Chief Deputy Doran advised us that body-worn cameras used in the jail record continuously. When jail staff respond to disturbances or other notable incidents, the relevant recordings are labeled accordingly,

which may result in a longer retention period. Otherwise, jail BWC recordings are retained for a 90-day period.

While Minnesota Statute §13.825 Subd. 1(a) states that: "[t]his section [§13.825] applies to law enforcement agencies that maintain a portable recording system for use in investigations, or in response to emergencies, incidents and requests for service," §13.825 Subd. 1(b)(1) states that: "'portable recording system' means a device worn by a **peace officer** that is capable of both video and audio recording of the officer's activities and interactions with others or collecting digital multimedia evidence as part of an investigation" [emphasis added].

In our opinion, BWC data created by non-sworn jail staff fall outside the scope of §13.825; consequently, we have not reviewed the Sherburne County Jail written BWC policy and do not express an opinion on its compliance with that statute, or with Minnesota Statute §626.8473, which incorporates §13.825 Subd. 1 by reference.

Data Sampling

Rampart selected a random sample of 132 calls for service (CFS) from which to review any available BWC recordings created by sworn personnel. It should be noted that not every call will result in a deputy activating his or her BWC. For example, a deputy 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 SCSO records.

Rampart selected a second random sample of 132 jail ICRs from which to review any available BWC recordings. Because BWCs used in the Sherburne County Jail record continuously, BWC data is likely to be created for every jail ICR. As noted above, however, because the audit covers a period of two years, this may exceed the retention period for some of the incidents for which BWC data was created. The auditor reviewed the retained BWC videos to verify that this data was accurately documented in Sherburne County Jail records.

Audit Conclusions

In our opinion, the Sherburne County Sheriff's Office's Body-Worn Camera Program is substantially compliant with Minnesota Statutes §13.825 and §626.8473.

Daniel E. Gazelka

Rampart Defense LLC

11/18/2022

APPENDIX A:

SHERBURNE COUNTY SHERIFF'S OFFICE SHERIFF'S OFFICE POLICY AND PROCEDURE MANUAL 703 Revised: 06/14/2021 Title: USE OF BODY-WORN CAMERAS Pages: 7 703.1 PURPOSE AND SCOPE The primary purpose of using body-worn-cameras (BWCs) is to capture evidence arising from police citizen encounters. This policy sets forth guidelines governing the use of BWCs and administering the resulting data. Compliance with these guidelines is mandatory, but it is recognized that deputies must also attend to other primary duties and the safety of all concerned, sometimes in circumstances that are tense, uncertain, and rapidly evolving. This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The sheriff or sheriff's designee may supersede this policy by providing specific instructions for BWC use to individual deputies, or providing specific instructions pertaining to particular events or classes of events, including but not limited to political rallies and demonstrations. The sheriff or designee may also provide specific instructions or standard operating procedures for BWC use to deputies assigned to specialized details, such as carrying out duties in courts or guarding prisoners or patients in hospitals and mental health facilities. 703.2 POLICY It is the policy of this office to authorize and require the use of department-issued BWCs as set forth below, and to administer BWC data as provided by law. 703.3 DEFINITIONS OF PHRASES 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 General Records Retention Schedule for Minnesota Counties. Law Enforcement-Related Information - 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 - 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 deputy. General Citizen Contact - 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 - 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 - A video recording resulting from a deputy'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 deputies were engaged in conversations of a non-business, personal nature with the expectation that the conversation was not being recorded. Test Recording Footage - A momentarily check of the BWC system conducted by a deputy to ensure the system is functioning correctly. Official Duties - For purposes of this policy, means that the deputy is on duty and performing authorized law enforcement services on behalf of this office. 703.4 USE AND DOCUMENTATION (a) Deputies 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 office. (b) Deputies who have been issued BWCs shall operate and use them consistent with this policy. Deputies shall make sure their BWC is working properly at the beginning of each shift. Deputies noting a malfunction shall promptly report the malfunction to the deputy's supervisor and shall document the malfunction with an ICR. Supervisors shall take prompt action to address malfunctions and document the steps taken in the ICR. (c) Deputies should wear their issued BWCs on their uniform shirt or jacket (if worn) in a position near their upper chest area. (d) Deputies must document BWC use and non-use as follows: 1. Whenever a deputy makes a recording, the existence of the recording shall be documented in an incident report if a case is generated or in the CAD notes if only a call is generated. 2. Whenever a deputy fails to record an activity that is required to be recorded under this policy or captures only a part of the activity, the deputy must document the circumstances and reasons for not recording in a supplement report to the original ICR if a case is generated, or in the CAD notes if only a call is generated. Supervisors shall review these reports and initiate any corrective action deemed necessary. (e) The sheriff's office 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 deputies; 3. The total amount of recorded BWC data collected and maintained; and 4. This policy, together with the Records Retention Schedule. 703.5 GENERAL GUIDELINES FOR RECORDING (a) Deputies 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 stop of 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 703.4(d)(2). (b) Deputies have discretion to record or not record general citizen contacts. (c) Deputies 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 deputy 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, deputies shall state the reasons for ceasing the recording on camera before deactivating their BWC. If circumstances change, deputies shall reactivate their cameras as required by this policy to capture information having evidentiary value. A statement on camera such as, "Everything has settled down and the action appears to be over" should often suffice as a statement of reasons for stopping to record. (e) Deputies shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy, except as allowed in 703.6 (c). (f) Notwithstanding any other provision in this policy, deputies 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. 703.6 SPECIAL GUIDELINES FOR RECORDING Deputies 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. (c) To momentarily mute the BWC microphone for the purpose of strategic consultation amongst deputies. In addition: (a) Deputies 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. (b) Deputies need not use their BWC 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. In-squad cameras will suffice for these types of transports. Deputies should not record with BWC's 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. Deputies may want to restart BWC at the time subject is removed from the car and transferred to the custody of another. In addition, for Transport/Court Security functions: (a) Deputies shall activate their BWCs when responding to an assigned call for service or when handling a self-initiated call for service such as a traffic stop, walk-in complaint, or any other self discovered activity requiring involvement or interaction. (b) Deputies shall not activate their BWCs within any correctional or secure detention facility. (c) Deputies shall not activate their BWCs in an active courtroom unless responding to a disturbance within the courtroom or taking someone into custody while in the courtroom and that person is either actively resisting or has become argumentative or noncompliant. Compliant forthwith arrests should not be recorded. (d) Deputies shall not activate their BWCs during the course of scheduled inmate or detainee medical appointments or medical guard details unless there is an active disturbance or hostile conduct involving the inmate or detainee. 703.7 DOWNLOADING AND LABELING DATA (a) Each deputy using a BWC is responsible for assuring the proper transfer of the data from his or her BWC system during his or her shift without incurring overtime. The intent is to prevent an excessive buildup of data on the BWC DVR. However, if the BWC DVR contains data that is likely to be needed immediately for an ongoing criminal investigation or is of a serious nature, the deputy shall download the data prior to the end of his or her shift. (b) Deputies shall categorize the BWC data files by choosing the category that best describes the event within the provided menu options at the time of video capture. (c) Upon a data request, Records shall forward notification of the request to the investigating deputies. Deputies shall then make an attempt to identify those persons whose image may have been captured in the BWC video footage. The identity of these persons is important in order to comply with MGDPA requirements related to data subjects. This data should be documented and added to a narrative report or CAD notes. At times it will be impractical to identify every individual at a scene, but special attention should be given to identifying the following: Victims, undercover deputies, informants, mandated reporters, juvenile witnesses (if the nature of the event or activity justifies protecting their identity) and juvenile delinquents, and individual complainants. (d) School Resource Officers should transfer data each week or before end of shift if data is likely to be needed immediately for an investigation or is of a serious nature. 703.8 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 deputy who collected the data. 3. Any other deputy whose voice or image is documented in the data, regardless of whether that deputy 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. After an investigation is complete, BWC data are public if they document 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. After an investigation is complete, BWC data are public if they document the use of force by a peace officer that result 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 deputies 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. 703.8.1 ACCESS TO BWC DATA BY NON-EMPLOYEES Deputies shall refer members of the media or public seeking access to BWC data to the records supervisor who shall process the request in accordance with the MGDPA and other governing laws. In particular: (a) 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: 1. If the data was collected or created as part of an active investigation. 2. 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. (b) 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: 1. Data on other individuals in the recording who do not consent to the release must be redacted. 2. Data that would identify undercover deputies must be redacted. 3. Data on other deputies who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted. 703.8.2 ACCESS BY PEACE OFFICERS AND LAW ENFORCEMENT EMPLOYEES No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes: (a) Deputies 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. (b) 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. (c) 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. 703.8.3 OTHER AUTHORIZED DISCLOSURES OF DATA Deputies 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. Deputies 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: (a) 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. (b) BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law. 703.9 DATA SECURITY SAFEGUARDS The Sherburne County Sheriff's Office IS will provide storage designed to back up all recordings. (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) Deputies shall not intentionally edit, copy, alter, or erase any BWC recording unless otherwise expressly authorized by the sheriff or the sheriff's designee. (c) As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this office shall obtain an independent biennial audit of its BWC program. 703.10 AGENCY USE OF DATA (a) Each time a BWC video is reviewed within the WatchGuard, the employee shall note the reason why for auditing purposes. Until the WatchGuard system is updated to include a data field for this purpose, employees shall document the reason for viewing in the comment section of the call in ProPhoenix RMS (e.g. "Viewed BWC for monthly audit," "Viewed BWC for report writing purposes," etc). If a case has more than one BWC video file, employees shall identify each video file reviewed and list a reason for viewing them. (b) At least once a month, supervisors will randomly review BWC usage by each deputy to ensure compliance with this policy. (c) 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 deputy 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. (e) Deputies should contact their supervisors to discuss retaining and using BWC footage for training purposes. Deputy objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training deputies may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance. 703.11 DATA RETENTION (a) BWC data shall be retained for a minimum period of 90 days (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 a deputy. (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 period requested by the subject of up to 180 days. The office 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 office shall maintain an inventory of BWC recordings having evidentiary value. The inventory will be kept in the BWC management system. (h) The office will post this policy, together with its Records Retention Schedule, on its website. 703.12 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.