



INDEPENDENT AUDITOR'S REPORT

Osseo Police Department Body-Worn Camera Program



JANUARY 30, 2023
RAMPART DEFENSE LLC
P.O. Box 23 Clearbrook, MN 56634

Audit Overview and Recommendations

Dear Osseo City Council and Chief Mikkelson:

We have audited the body-worn camera (BWC) program of the Osseo Police Department (OPD) for the two-year period ended 10/14/2022. 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 Osseo Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On November 14, 2022, Rampart Defense LLC (Rampart) met with Chief Shane Mikkelson, who provided information about OPD'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 OPD's recordkeeping.

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

OPD 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 Mikkelson provided documentation showing that the public notification, comment and meeting requirements had been satisfied prior to the implementation of OPD's BWC program on October 15, 2020. Specifically, Chief Mikkelson furnished a copy of the minutes of the June 22, 2020, Osseo City Council meeting, at which he requested that the council schedule a public hearing to take comments from the public for the proposed BWC program and policy. The minutes noted that OPD also solicited

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 OPD, these terms may be used interchangeably in this report.

comments from the public via mail and email. Chief Mikkelson also furnished an agenda item request memo to the Osseo City Council, requesting that the council open the July 27, 2020, meeting for public comment about the proposed BWC policy and then consider adopting the policy. The memo discussed the results of a review of the policy by the Public Safety Committee and noted that Chief Mikkelson had also received comments from the public regarding the proposed BWC program via email and intended to read those at the city council meeting. Finally, Chief Mikkelson furnished a copy of the July 27, 2020, Osseo City Council meeting minutes, which noted that he had read the email comments from the public into the record. He also clarified for the council the policy provision allowing officers to discontinue recording under certain circumstances. A public hearing was called during the meeting to receive questions from the public regarding the proposed body camera policy. There were no additional questions or comments. After the public hearing was closed, the city council voted to approve the body-worn camera policy as written. Copies of these documents have been retained in Rampart's audit files.

Rampart staff verified that the BWC policy was accessible from the Osseo Police Department's webpage at the time of our audit.

OPD BWC WRITTEN POLICY

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

OPD BWC Data Retention

OPD's data retention 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." The policy also includes an itemized list of retention periods for different categories of BWC data. These guidelines meet or exceed the requirements specified for each category of BWC data enumerated in §13.825 Subd. 3.

OPD employs eight (8) Getac body-worn cameras and utilizes Getac's cloud-based service for BWC data storage. OPD manages BWC data retention through automated retention settings in the Getac 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.

OPD'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, OPD's written BWC policy is compliant with respect to applicable data retention requirements.

OPD BWC Data Destruction

As discussed above, OPD'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), and notes that it has signed CJIS management agreements with 45 of the 50 U.S. states, including Minnesota, to verify compliance with state CJIS requirements.

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

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

OPD BWC Data Access

Any request for access to BWC data by data subjects or the media would be made to the Osseo Police Department Office Manager, who is responsible for reviewing and fulfilling each request in accordance with the provisions of §13.825 Subd. 4(b). Chief Mikkelson is also notified of any requests.

According to OPD's BWC policy, BWC data are shared with other law enforcement agencies "only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure." All such requests must be made to OPD Office Manager and are fulfilled via an expiring email link. Requests from the Hennepin County Attorney's Office are made by email and fulfilled using the same expiring email link process. Requests from the Osseo City Attorney's Office are also made via email but are fulfilled through a secure shared drive.

We recommend that OPD obtain a written acknowledgment from each requesting agency acknowledging its responsibilities under §13.825 Subd. 7 and 8. A copy of these acknowledgments should be maintained on file.

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

OPD BWC Data Classification

OPD 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.

OPD BWC Internal Compliance Verification

OPD's 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 Mikkelson advised us that he conducts random checks on a near-daily basis to monitor for compliance with both BWC usage and access requirements.

In our opinion, OPD's BWC policy meets the compliance and disciplinary requirements specified in §626.8473 Subd. 8.

OPD BWC Program and Inventory

OPD currently possesses eight (8) Getac body-worn cameras.

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

While OPD does not maintain a separate log of BWC deployment or use, Chief Mikkelson advised us that deployment can be determined based on a review of OPD payroll records. Actual BWC use would be determined based on the creation of BWC data.

As of 11/14/2022, OPD maintained 829 GB of BWC data.

OPD BWC Physical, Technological and Procedural Safeguards

OPD BWC data are initially recorded to an internal hard drive in each officer's BWC. Those files are then transferred through an automated upload process to Getac's cloud-based servers. As discussed earlier in this report, Getac utilizes Microsoft's Azure Government to ensure CJIS compliance.

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

As noted above, requests by other law enforcement agencies for OPD BWC data are submitted to the OPD Office Manager and are fulfilled via expiring email link. A similar method is employed to submit OPD BWC data to the Hennepin County Attorney's Office, while the Osseo City Attorney's Office receives video through a secure shared drive.

Enhanced Surveillance Technology

OPD currently employs a BWC system 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 OPD 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 ICRs 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 OPD records.

Rampart Defense, LLC

Audit Conclusions

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


A handwritten signature in black ink, appearing to read "Daniel E. Gazelka", is written over a solid horizontal line.

Daniel E. Gazelka

Rampart Defense LLC

1/30/2023

Appendix A:

	<h2>Osseo Police Department Policy Manual</h2>				
General Number	187	By the order of:	Chief Shane Mikkelson		
Policy:	Body-Worn Cameras				
Effective Date:	08/26/2020	Review Date:		Revision Date	

Purpose

The primary purpose of using body-worn-cameras (BWCs) is to promote transparency and accountability and build trust, enhance officer and public safety, and 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.

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.

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 instruction 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 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.

Definitions

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

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

2. **Records Retention Schedule** refers to the General Records Retention Schedule for Minnesota Cities.
3. **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.
4. **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.
5. **General citizen contact** means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial. 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.
6. **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 that other verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, shouting, or encounters in which a citizen “demands” to be recorded.
7. **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 conversation of a non-business, personal nature with the expectation that the conversation was not being recorded.
8. **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.

Operational Objectives

Operational objectives include:

- a) Promote transparency and accountability and build community trust
- b) Enhance officer and public safety

- c) Collect evidence for use in criminal investigation and prosecution
- d) Assist in resolving complaints against personnel
- e) Deter criminal activity and uncooperative behavior during police contacts
- f) Enhance the officer's ability to document and review statement and actions for internal reporting requirements and courtroom preparation
- g) Promote additional information for training
- h) Utilize best practices in the rapidly evolving field of law enforcement.

Issuance of Body-Worn Cameras (BWC)

BWC's will be mandatory for uniformed officers assigned to the Patrol Division for daily use. Furthermore, BWC will be mandatory for non-uniformed personnel when they don a "raid vest" or body armor. Uniformed officers performing contacte4d overtime services will wear BWC's as part of their uniform. Cameras will be made available to all officers, such as investigators, for instances when the officer reasonably believes he/she will be in contact with the public, and the use of a BWC will enhance the officer's ability to achieve the operational objectives outlined above.

Training

Users of the BWC system will be trained in its operation.

Use and Documentation

1. 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.
2. Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall properly charge the camera battery when not in use and shall assure the camera is working properly on a daily basis. 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 steps taken in writing.

3. Officers should wear their issued BWCs at the location of their body and in the manner specified in training.
4. Officers must document BWC use and non-use as follows:
 - a. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report, ICR, CAD record, or relevant department form.
 - b. 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, ICR, CAD record, or relevant department form. Supervisors shall review these reports and initiated any corrective action deemed necessary.
5. The department will maintain the following records and documents relating to BWC use, which are classified as public data:
 - a. The total number of BWCs owned or maintained by the agency.
 - b. A daily record of the total number of BWCs deployed and used by officers.
 - c. The total amount of recorded BWC data collected and maintained.
6. This policy, together with the Record Retention Schedule.

General Guidelines for Recording

1. 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
 - Traffic stops
 - Foot or vehicle pursuits,
 - Terry stop of a motorist or pedestrian,
 - Search,
 - Seizure,
 - Arrest,
 - Use of force,
 - Adversarial contact,
 - Transports,
 - Other activities likely to yield information having evidentiary value
 - Officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, in such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, (see E above)

2. BWC are not intended to replace the need for a detailed incident report or other reporting requirements.
3. Officers have the discretion to record or not record general citizen contacts.
4. Officers have no affirmative duty to inform people that a BWC is operated or that the individuals are being recorded.
5. 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.
6. Recording (and/or the audio track of a recording) may be temporarily ceased, but officers shall not intentionally alter, block or tamper with the BWC's audio or visual recording functionality to defeat the purposes of this policy.
7. 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 the 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.

Special Guidelines for Recording

Officers should be mindful that BWC's are not intended to replace equipment issued to department personnel to take a recorded statement of suspects, victims and/or witnesses. Likewise, BWC's are not intended to replace equipment to photograph evidence, crime scenes, etc. Officers may, in the exercise of sound discretion, determine:

1. 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.
2. 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.

3. Officers shall use the BWCs and/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 and adversarial encounter or use-of-force incident.

Downloading and Categorizing Data

1. Video files shall be maintained in an approved storage location, such as a server, storage device, cloud storage, website, or other approved secure storage media, authorized by the Chief of Police. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera by the end of that officer's shift. However, if the officers are 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.
2. Officers shall categorize the BWC data files at the time of video capture or transfer to storage and should consult with a supervisor if in doubt as to the appropriate labeling. Officers should assign as many of the following labels as are applicable to each file:

- a. From BWC
 1. ICR/Other 90-day retention
 2. Citation 3-year retention
 3. Arrest/RTR(Response to resistance) 7-year retention
 4. Permanent Permanent retention
- b. From In-Car System
 1. ICR/Other 90-day retention
 2. Citation 3-year retention
 3. Arrest/RTR (response to Resistance) 7-year retention
 4. Squad Check 90-day retention
 5. Permanent Permanent retention

Administering Access to BWC Data

1. Data subjects: Under Minnesota law, the following are considered data subjects for the purpose of administering access to BWC data:
 - a. Any person or entity whose image or voice is documented in the data.
 - b. The officer who collected the data.
 - c. 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.

2. 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:
 - a. BWC data pertaining to people is presumed private, as is BWC data pertaining to business or other entities.
 - b. Some BWC data is classified as confidential
 - c. Some BWC data is classified as public

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.

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 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.

Access to BWC data by non-employees

Officers shall refer members of the media or public seeking access to BWC data to the Chief of Police, 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 himself/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.

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 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 to report, giving a statement, or providing testimony about the incident.
2. 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.

Other authorized disclosure 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 screenshots, 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.

Data Security Safeguards

1. 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.
2. Officers shall not intentionally edit, alter, erase, or copy any BWC recording unless otherwise expressly authorized by the Chief or the Chief's designee.
3. Unless authorized by the Chief of Police, officers are not allowed to store or bring their BWC's home during off-duty hours.
4. 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.

Agency Use of Data

1. 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.
2. Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.
3. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officer objections to preserving or using certain footage from 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.

Data Retention

1. All BWC data shall be retained for a minimum period of 90days. There are no expectations for erroneously recorded or non-evidentiary data.
2. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of any animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.
3. Certain kinds of BWC data must be retained for six years:
 - a. 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 supervisor review.
 - b. Data documenting circumstances that have given rise to a formal complaint against an officer.
4. 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.
5. Subject to Part F (below), all other BWC forage that is classified as “ICR/Other or Squad Check” or is not maintained for training shall be destroyed after 90 days.
6. 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 for 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.
7. The department shall maintain an inventory of BWC recordings having evidentiary value.
8. The department will post this policy and a link to the Record Retention schedule on the city website.

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.

Policy and Program Evaluation

Rampart Defense, LLC

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.