



# INDEPENDENT AUDITOR'S REPORT

---

Wadena Police Department



MAY 25TH, 2023  
RAMPART DEFENSE LLC  
P.O. Box 23 Clearbrook, MN 56634

## **Audit Overview and Recommendations**

Dear Wadena City Council and Chief Plautz:

We have audited the body-worn camera (BWC) program of the Wadena Police Department (WPD) for the period of 3/15/2021 - 3/14/2023. 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 Wadena Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On April 25, 2023, Rampart Defense LLC (Rampart) met with Chief Naomi Plautz and Sgt. Brandon Pearson, who provided information about WPD'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 WPD's recordkeeping.

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

### **WPD 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.

Sgt. Pearson provided Internet links to the following documents posted on the City of Wadena website as evidence that WPD had met these requirements:

1. A notice announcing a public hearing to be held during the March 9, 2021, Wadena City Council meeting to discuss the proposed BWC program and policy. The notice included an Internet link to the draft BWC policy, as well as instructions for obtaining a printed copy. It also included an invitation and instructions for providing written comments in advance of the meeting or oral comments at the meeting.

---

<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 WPD, these terms may be used interchangeably in this report.

2. An Internet link to the March 9, 2021, Wadena City Council Meeting Minutes, which note the opening of a public comment period during the regularly-scheduled city council meeting for the purpose of discussing the proposed BWC policy and program.

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

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

Sgt. Pearson furnished to Rampart a link to WPD's BWC policy, which was posted on the Wadena Police Department's website. Rampart verified that this link worked at the time of receipt. We noted that the policy link was prominently displayed on the WPD homepage, along with a second link to the BWC retention schedule. In our opinion, Wadena Police Department is compliant with the requirements of §626.8473 Subd. 3(a).

#### **WPD BWC WRITTEN POLICY**

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

### **WPD BWC Data Retention**

The Data Retention section of the WPD BWC policy sets forth retention periods that meet or exceed the requirements for each category of BWC data enumerated in §13.825 Subd. 3(b).

Clause (A) of the Data Retention section of the WPD BWC policy states that “[a]ll Portable Recording Devices data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.”

Clause (B) of the Data Retention section of the WPD BWC policy specifies a minimum retention period of one year for data documenting the discharge of a firearm under circumstances described in §13.825 Subd. 3(b)(1)(i).

Clause (C) of the Data Retention section of the WPD BWC policy specifies a minimum retention period of six years for data documenting use of force resulting in substantial bodily harm as described in §13.825 Subd. 3(b)(1)(ii), as well as for data documenting incidents giving rise to a formal complaint against an officer as described in §13.825 Subd. 3(b)(2).

Clause (D) of the Data Retention section of the WPD BWC policy 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.”

WPD employs Watchguard body-worn cameras and utilizes a secure server that is shared with the Wadena County Sheriff’s Office and managed by Wadena County Information Technology staff. WPD manages BWC data retention through automated retention settings in Watchguard’s Evidence Library video management software. The retention period for each video is determined by the data classification assigned at the time of upload; however, this retention period can be adjusted as needed.

WPD’s BWC policy states that “[e]ach officer using a Portable Recording Devices is responsible for transferring or assuring the proper transfer of the data from his or her camera to upload to the Watchguard system by the end of that officer’s shift.” This is accomplished by physically docking the BWC either in the officer’s squad or at the Wadena Police Department in order to upload the data via a wireless connection. Officers are required to assign the appropriate data label or labels to each file at the time of capture or transfer to storage.

In our opinion, WPD’s written BWC policy is compliant with respect to the applicable data retention requirements.

### **WPD BWC Data Destruction**

As discussed above, WPD’s BWC data are stored on a secure server managed by Wadena County IT personnel, with data retention and deletion schedules managed automatically through the Evidence Library video management software based on the assigned data classification of each video.

Rampart previously audited the Wadena County Sheriff’s Office’s (WCSO) BWC program on March 17, 2022. At that time, WCSO personnel advised us that WCSO BWC data are stored on a secure on-site server and backed-up to a secure, remote server in a second county-owned facility, with data retention

and deletion schedules managed automatically based on the data classification assigned to each video. Deleted BWC data are overwritten by newly created files. In addition, at the time it is retired from service, any WCSO-owned physical hard drive used to store BWC data will have all data deleted prior to being destroyed by physical means. Because WPD data are stored on the same servers, the same destruction processes apply to that data as well.

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

### **WPD BWC Data Access**

WPD's BWC policy states that officers shall refer "members of the media or public seeking access to Portable Recording Devices data to the Chief or designee, who shall process the request in accordance with the MGDPA [Minnesota Government Data Practices Act] and other governing laws." BWC recordings are shared with members of the public via physical media such as DVD. Such recordings are subject to redaction as described in §13.825 Subd. 4(b).

WPD's BWC policy also states that BWC data "may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure." In addition, BWC data "shall be made available to prosecutors, courts, and other criminal justice entities as provided by law."

Sgt. Pearson advised us that Wadena Police Department has a written agreement in place with the Wadena County Sheriff's Office regarding WCSO access to WPD BWC data. BWC data are shared with prosecutors via physical media such as DVDs.

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

### **WPD BWC Data Classification**

WPD's BWC Policy states that "Portable Recording Devices data is presumptively private," and further states that "Portable Recording Devices recordings are classified as private data about the data subjects unless there is a specific law that provides differently." Active criminal investigation data are classified as confidential. WPD BWC Policy also identifies certain categories of BWC data that are public.

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

### **WPD BWC Internal Compliance Verification**

The WPD BWC Policy Agency Use of Data section states that:

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

In addition, supervisors and other assigned personnel may access Portable Recording Devices 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.

Sgt. Pearson advised us that he reviews three (3) videos per officer each month. All reviews are logged and subject to audit by WPD administration.

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

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

### **WPD BWC Program and Inventory**

WPD currently possesses 10 Watchguard body-worn cameras, including one retained as a spare.

The WPD 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.

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

As of the time of the audit, WPD maintained 2,364 BWC data files.

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

WPD BWC data are initially recorded to a hard drive in each officer's BWC. Prior to the end of each shift, the officer places his or her BWC in a docking station either in his or her squad or at WPD. Any BWC data are then uploaded automatically to a secure server that is shared with the Wadena County Sheriff's Office. That server is backed up to a second secure server to guard against the accidental loss of data. Wadena County IT personnel are responsible for managing data security safeguards for those servers. Rampart previously reviewed the Wadena County Sheriff's Office's physical, technological and procedural safeguards as part of our March 17, 2022, audit of that agency's BWC program.

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

### **Enhanced Surveillance Technology**

WPD 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 WPD should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses.


### **Data Sampling**

Rampart selected a random sample of 132 calls for service (CFS) from which to review any available BWC recordings. It should be noted that not every call will result in an officer activating his or her BWC. For example, an officer who responds to a driving complaint but is unable to locate the suspect vehicle would be unlikely to activate his or her BWC. It should also be noted that because this audit covers a period of two years, while most BWC data is only required to be retained for 90 days, there is a significant likelihood that the sample population will include calls for which BWC data was created, but which has since been deleted due to the expiration of the retention period. The auditors reviewed the retained BWC videos to determine whether this data was accurately documented in WPD records.

All reviewed videos were properly identified by CFS number.

### **Audit Conclusions**

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



Daniel E. Gazelka

Rampart Defense LLC

5/25/2023

## APPENDIX A:

Page 1 of 12 Policy 409-1 Effective Date: March 12, 2021 Subject: Portable Recording Devices To: All Personnel From: Chief Naomi J. Plautz PURPOSE The primary purpose of using Portable Recording Devices is to capture evidence arising from police/citizen encounters. This policy sets forth guidelines governing the use of Portable Recording Devices 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 Portable Recording Devices as set forth below, and to administer Portable Recording Devices data as provided by law. SCOPE This policy governs the use of Portable Recording Devices 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 Portable Recording Devices 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. City of OFFICE OF THE POLICE DEPARTMENT 121 COLFAX AVENUE SE, WADENA, MN 56482 Page 2 of 12 The chief or designee may also provide specific instructions or standard operating procedures for Portable Recording Devices 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 and words have special meanings as used in this policy: A. MGDPA or Data Practices Act refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq. B. Records Retention Schedule refers to the General Records Retention Schedule for Minnesota Cities. C. Law enforcement-related information means information captured or available for capture by use of a Portable Recording Devices 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. Page 3 of 12 G. Unintentionally recorded footage is a video recording that results from an officer's inadvertence or neglect in operating the officer's Portable Recording Device, provided that no portion of the resulting recording has evidentiary value. Examples of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms, restrooms, and recordings made while officers were engaged in conversations of a non-business, personal nature with the expectation that the conversation was not being recorded. H. Official duties, for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this agency. USE AND DOCUMENTATION A. Officers may use only department-issued Portable Recording Devices 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 Portable Recording Devices shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued Portable Recording Devices 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 Portable Recording Devices at the location on their body and in the manner specified in training. D. Officers must document Portable Recording Devices use and non-use as follows: 1. Whenever an officer makes a recording, the existence of the recording shall be documented in an incident report. 2. Whenever an officer fails to record an activity that is required to be recorded under this policy, or fails to record for the entire duration of the activity, the officer must document the circumstances and reasons for not recording in an incident report. Supervisors shall review these reports and initiate any corrective action deemed necessary. Page 4 of 12 E. The department will maintain the following records and documents relating to Portable Recording Devices use, which are classified as public data: 1. The total number of Portable Recording Devices owned or maintained by the agency; 2. A daily record of the total number of Portable Recording Devices actually deployed and used by officers and, if applicable, the precincts in which they were used; 3. The total amount of recorded Portable Recording Devices data collected and maintained; and 4. This policy, together with the Records Retention Schedule. GENERAL GUIDELINES FOR RECORDING A. Officers shall activate their Portable Recording Devices when responding to all calls for service and during all law enforcement-related encounters and activities, including but not limited to pursuits, Terry stops of motorists or pedestrians, arrests, searches, suspect interviews and interrogations, and during any police/citizen contacts that becomes adversarial. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, part (D)(2) (above). B. Officers have discretion to record or not record general citizen contacts. C. Officers have no affirmative duty to inform people that a Portable Recording Devices is being operated or that the individuals are being recorded. D. Once activated, the Portable Recording Devices 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 Portable Recording Devices. If circumstances change, officers shall reactivate their cameras as required by this policy to capture information having evidentiary value. Page 5 of 12 E. Officers shall not intentionally block the Portable Recording Device's audio or visual recording functionality to defeat the purposes of this policy. F. Notwithstanding any other provision in this policy, officers shall not use their Portable Recording Devices 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. SPECIAL GUIDELINES FOR RECORDING Officers may, in the exercise of sound discretion, determine: A. To use their Portable Recording Devices 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 Portable Recording Devices 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, Portable Recording Devices shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue. D. Officers shall use their Portable Recording Device to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails, but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident. Page 6 of 12

**DOWNLOADING AND LABELING DATA**

A. Each officer using a Portable Recording Devices is responsible for transferring or assuring the proper transfer of the data from his or her camera to upload to the Watchguard system by the end of that officer's shift. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the officer's Portable Recording Device and assume responsibility for transferring the data from it. B. Officers shall label the Portable Recording Devices data files at the time of capture or transfer to storage, and should consult with a supervisor if in doubt as to the appropriate labeling. Officers should assign as many of the following labels as are applicable to each file: 1. Test/Delete 2. Motorist Assist 3. Civil Process 4. Traffic Warning 5. Emergency Operation 6. Other/Non Traffic 7. Assist Other Agency 8. Suspicious Vehicle/Behavior 9. Traffic Citation 10. Arrest 11. DWI 12. Pursuit 13. Interview 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. Page 7 of 12

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.

**ADMINISTERING ACCESS TO PORTABLE RECORDING DEVICES**

**DATA**

A. Data subjects. Under Minnesota law, the following are considered data subjects for purposes of administering access to Portable Recording Devices 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 Page 8 of 12

B. Portable Recording Devices data is presumptively private. Portable Recording Devices recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result: 1. Portable Recording Devices data pertaining to people is

presumed private, as is Portable Recording Devices data pertaining to businesses or other entities. 2. Some Portable Recording Devices data is classified as confidential (see C. below). 3. Some Portable Recording Devices data is classified as public (see D. below). C. Confidential data. Portable Recording Devices 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 Portable Recording Devices data is public: 1. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous. 2. Data that documents the use of force by a peace officer that results in substantial bodily harm. 3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted. In addition, any data on undercover officers must be redacted. 4. Data that documents the final disposition of a disciplinary action against a public employee. However, if another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other classification. For instance, data that reveals protected identities under Minn. Stat. § 13.82, subd. 17 (e.g., certain victims, witnesses, and others) should not be released even if it would otherwise fit into one of the public categories listed above. E. Access to Portable Recording Devices data by non-employees. Officers shall refer members of the media or public seeking access to Portable Recording Devices data to the Chief or designee, who shall process the request in accordance with the MGDPA and other governing laws. In particular: Page 9 of 12 1. An individual shall be provided with access and allowed to review recorded Portable Recording Devices 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 Portable Recording Devices data except for legitimate law enforcement or data administration purposes: 1. Officers may access and view stored Portable Recording Devices 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 Portable Recording Devices data in the manner provided within the database at the time of each access. Agency personnel are prohibited from accessing Portable Recording Devices data for non-business Page 10 of 12 reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading Portable Recording Devices data recorded or maintained by this agency to public and social media websites. 3. Employees seeking access to Portable Recording Devices 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 Portable Recording Devices footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time

to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individual identities that are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition, 1. Portable Recording Devices 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. Portable Recording Devices data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law. DATA SECURITY SAFEGUARDS A. The data security safeguards will be handled by the Wadena County IT department personnel. B. Access to Portable Recording Devices data from city or personally owned and approved devices shall be managed in accordance with established city policy. C. Officers shall not intentionally edit, alter, or erase any Portable Recording Devices 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 Portable Recording Devices program. Page 11 of 12 AGENCY USE OF DATA A. At least once a month, supervisors will randomly review Portable Recording Devices usage by each officer to whom a Portable Recording Devices is issued or available for use, to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required. B. In addition, supervisors and other assigned personnel may access Portable Recording Devices 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 Portable Recording Devices data as evidence of misconduct or as a basis for discipline. D. Officers should contact their supervisors to discuss retaining and using Portable Recording Devices 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 Portable Recording Devices data with trainees for the purpose of providing coaching and feedback on the trainees' performance. DATA RETENTION A. All Portable Recording Devices 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 Portable Recording Devices data must be retained for six years: Page 12 of 12 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 Portable Recording Devices footage that is classified as nonevidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days. F. Upon written request by a Portable Recording Devices data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. The agency will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received. G. The department shall maintain an inventory of Portable Recording Devices recordings having evidentiary value. H. The department will post this policy, together with a link to its Records Retention Schedule, on its website, Wadena.org. COMPLIANCE 1. Supervisors shall monitor for compliance with this policy. The unauthorized access to or

Rampart Defense, LLC

disclosure of Portable Recording Devices data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. § 13.09.