Audit of Cannon Falls Police

Department Body Worn Cameras

September, 2020

Executive Summary

The audit found the BWC program is effective and operating as originally intended. Cannon Falls Police Department (CFPD) successfully implemented the use of BWC at a time when there was little direction from the state. CFPD recognized the value of BWCs prior to national discussions about the use of BWCs. Now state laws governing the use of body-worn cameras provides significant guidance through the use of policies. However, the ability to fully manage this infrastructure without management software is restricting CFPD's efforts to self-audit.

The CFPD trains new hires in the BWC policy and all officers on an ongoing basis. However, there could be opportunities for improvement with the addition of video management software. The current storage of video is not accomplished with management software but with standard computer file management practices. Files uploaded from the cameras are simply loaded into the appropriate folder. Once there, access to the files are limited for supervisors and staff of CFPD. Video management software should be employed so state video retention dates could be automated to save labor.

Although not required, some recommendations include;

- *Publish the policy on web page so the public can find it easier*
- *Utilizing program file labelling to protect categories of vulnerable individuals*

Table of Contents

Background

The audit was ordered at the beginning of 2019. The time period reviewed is January 2017 to September 2020.

Cannon Falls Police department began using BWC in 2011. The department has 17 body cameras and 12 functional cameras and are assigned to Officers by badge#. BWC video is stored on the internal city network. A network attached storage device has all raw footage from the BWCs. CFPD policy dictates when footage should be uploaded.

Current storage for BWCs includes 451 folders containing 1936 files. Files are stored by badge number and day

Objective, Scope and Approach

Objective

The objective of the audit was to determine whether body worn cameras and respective programs were being used and executed in accordance with statutes and policies, and were adequately designed, administered and monitored.

A review of compliance with Minnesota Statutes was part of this audit.

Scope

The scope included:

- CFPD policies on BWC use and resulting data storage and use.
- CFPD training process.
- Hardware and software used by CFPD in its BWC program.
- Data generated by BWCs.

Approach

To accomplish audit objectives, Internal Audit:

- Reviewed Minnesota statutes.
- Reviewed CFPD policy and training process.
- Discussed program functionality with CFPD staff.
- Discussed BWC software functionality with staff.
- Evaluated data access controls.

Audit Results and Recommendations

Audit results

CFPD use of BWCs is in compliance with state statutes. The use of city policy is the prime tool for maintaining this compliance.

Audit Recommendations

The BWC program needs a management software program to include the necessary hardware and software in order to fully create the ability to self audit and easier management of compliance with statutes. With the correct tools, requests for access, preparing data for release, and providing for independent biennial will be handled easier.

State Statute regarding BWC broken down

13.825 Subd 2 (a)	Data collected by a portable recording system are private data on individuals or nonpublic data.	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (1)	Data that document the discharge of a firearm by a peace officer in the course of duty other than during training and the killing of an animal that is sick, injured, or dangerous (section 626.553 Subd. 2) are public.	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (1)	Data that document the use of force by an officer that results in substantial bodily harm (bodily injury which involves a temporary but substantial disfigurement, or which causes a temporary but substantial loss or impairment of the function of any bodily member or organ, or which causes a fracture of any bodily member), are public.	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (2)	Data are public if a subject of the data requests it be made accessible to the public.	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (2) i	Data on a subject who is not a peace officer and who does not consent to the release must be redacted.	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (2) ii	Data on a peace officer whose identity is protected (undercover law enforcement officer) must be redacted.	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (3)	Portable recording system data that are active criminal investigative are confidential or protected nonpublic and governed the Criminal Investigative Data statute (section 13.82, subdivision 7).	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (3)	Portable recording system data that are inactive criminal investigative data are public as governed by this data classification section.	Reviewed the BWC policy and identified the current policy does cover data classification for inactive criminal investigations, as required per legislative requirements.	In compliance
13.825 Subd 2 (a) (4)	Data is public regarding the final disposition of any disciplinary action together with the specific reasons for the action and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of the public body.	Reviewed the BWC policy and identified the current policy does cover data classification for disciplinary action.	In compliance

13.825 Subd 2 (a) (5)	Data that are not public data under other provisions of this chapter retain that classification.	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (5) (b)	A law enforcement agency may redact or withhold access to portions of data that are public under this subdivision if those portions of data are clearly offensive to common sensibilities.	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (5) (c)	Tennessen warning (Section 13.04, subdivision 2) does not apply to collection of data classified by this subdivision.	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (5) (d)	The person bringing the action to challenge a determination to withhold access to portion of data must give notice of the action to the law enforcement agency and subjects of the data, if known.	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (5) (d)	The law enforcement agency must give notice to other subjects of the data, if known, who did not receive the notice from the person bringing the action	Reviewed the BWC policy.	In compliance
13.825 Subd 2 (a) (5) (d)	The right of a defendant in a criminal proceeding to obtain access to portable recording system data under the Rules of Criminal Procedure is not affected by section related to withholding access or redacting portion of data that is clearly offensive to common sensibilities.	Reviewed the BWC policy.	In compliance
13.825 Subd 3 (a)	Body cam data that are not active or inactive criminal investigative data must be retained for at least 90 days.	Reviewed the BWC policy.	In compliance
13.825 Subd 3 (b)	Body cam data must be destroyed according to the agency's record retention schedule approved pursuant to section 138.17 (retention schedule approved by the head of the governmental unit or agency having custody of the records and the MN Records Disposition Panel)	Evaluated the BWC policy and confirmed data is destroyed per CJIS standards once retention schedule is met.	In compliance
13.825 Subd 3 (b)	Body cam data must be retained for at least one year if they document an incident where an officer discharges a firearm in the course of duty other than the exceptions noted in section 626.553 Subd 2 (training and the killing of an animal that is sick, injured, or dangerous,)	Reviewed the BWC policy.	In compliance
13.825 Subd 3 (1)	Body cam data must be retained for at least one year if they document the use of force by an officer that results in substantial bodily harm.	Reviewed the BWC policy.	In compliance
13.825 Subd 3 (2)	Body cam data must be retained for at least one year if a formal complaint is made against an officer related to an incident.	Reviewed the BWC policy.	In compliance
13.825 Subd 3 (c)	If a subject of the data submits a written request to retain the recording, the data must be retained for the time period requested, of up to an additional 180 days beyond the applicable retention period.	Reviewed the BWC policy.	In compliance

13.825 Subd 3 (c)	The law enforcement agency shall notify the requester that the recording will be destroyed when the requested time elapsed unless a new request is made.	Reviewed the BWC policy.	In compliance
13.825 Subd 3 (d)	A government entity may retain a recording for as long as reasonably necessary for possible evidentiary or exculpatory use related to the incident with respect to which the data were collected.	Reviewed the BWC policy.	In compliance
13.825 Subd 4 (b)	An individual who is the subject of portable recording system data can have access to the data, including data on other individuals who are the subject of the recording.	Reviewed the BWC policy.	In compliance
13.825 Subd 4 (b)	If the individual requests a copy of the recording, data on other individuals who do not consent to its release must be redacted from the copy.	Reviewed the BWC policy.	In compliance
13.825 Subd 4 (b)	The identity and activities of an on-duty peace officer engaged in an investigation or response to an emergency, incident, or request for service may not be redacted, unless the officer's identity is subject to protection under section 13.82, subdivision 17, clause (a) (when access to the data would reveal the identity of an undercover law enforcement officer).	Reviewed the BWC policy.	In compliance
13.825 Subd 5	A law enforcement agency that uses a portable recording system must maintain the following information, which is public data: (1) the total number of recording devices owned or maintained by the agency; (2) a daily record of the total number of recording devices actually deployed and used by officers and, if applicable, the precincts in which they were used; (3) the policies and procedures for use of portable recording systems required by section 626.8473; and (4) the total amount of recorded audio and video data collected by the portable recording system and maintained by the agency, the agency's retention schedule for the data, and the agency's procedures for destruction of the data.	Reviewed and confirmed the total number of recording devices owned by the agency, deployed and used by officers, and the total amount of data collected by the portable recording devices and maintained by the agency are all reportable.	In compliance
13.825 Subd 7 (a)	The chief officer of every state and local law enforcement agency that uses or proposes to use a portable recording system must establish and enforce a written policy governing its use.	Reviewed the BWC policy.	In compliance
Portable Recording Systems Adoption; Written Policy Required	The written policy must be posted on the agency's Web site, if the agency has a Web site.	Confirmed the current BWC policy is available on the Cannon Falls Police Department’s website.	In compliance

13.825 Subd 6	While on duty, a peace officer may only use a portable recording system issued and maintained by the officer's agency in documenting the officer's activities.	Reviewed the BWC policy.	In compliance
13.825 Subd 7 (b)	The responsible authority for a law enforcement agency must establish written procedures to ensure that law enforcement personnel have access to the portable recording system data that are not public only if authorized in writing by the chief of police, sheriff, or head of the law enforcement agency, or their designee, to obtain access to the data for a legitimate, specified law enforcement purpose.	Reviewed the Access control procedure for the CFPD BWC program and confirmed the documented procedures sufficiently meet the requirements defined in the legislation.	In compliance
13.825 Subd 8 (a)	Portable recording system data that are not public may only be shared with or disseminated to another law enforcement agency, a government entity, or a federal agency upon meeting the standards for requesting access to data as provided in subdivision 7	Reviewed the BWC policy.	In compliance
13.825 Subd 8 (b)	If data collected by a portable recording system are shared with another state or local law enforcement agency under this subdivision, the agency that receives the data must comply with all data classification, destruction, and security requirements of this section.	Reviewed the BWC policy.	In compliance
13.825 Subd 8 (c)	Portable recording system data may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by this section or other applicable law.	Reviewed the BWC policy.	In compliance
13.825 Subd 9 (a)	A law enforcement agency must maintain records showing the date and time portable recording system data were collected and the applicable classification of the data.	Reviewed the exported the body camera logs to satisfy legislative requirements.	In compliance
13.825 Subd 11 (a)	Within ten days of obtaining new surveillance technology that expands the type or scope of surveillance capability of a portable recording system device beyond video or audio recording, a law enforcement agency must notify the Bureau of Criminal Apprehension that it has obtained the new surveillance technology	Confirmed no other new surveillance technologies, beyond current capability.	In compliance
13.825 Subd 11 (b)	The notice must include a description of the technology and its surveillance capability and intended uses. The notices are accessible to the public and must be available on the bureau's Web site.	Confirmed no other new surveillance technologies, beyond current capability.	In compliance

626.8473 Subd 2	Section 626.8473 requires a law enforcement agency to allow for public comment and to create written policies and procedures before it purchases body cams or implements a body cam program. Such policies and procedures must be in place by January 15, 2017.	Reviewed documentation and confirmed a meeting for public comment input took place on December 6, 2016.	In compliance
626.8473 Subd 3	At a minimum, the written policy must incorporate the following:(1) the requirements of section 13.825 and other data classifications, access procedures, retention policies, and data security 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 under which 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;	Reviewed BWC documentation and confirmed the following requirements were present and complete in the written policy, procedure	In compliance
626.8473 Subd 3 (8)	Procedures to ensure compliance and address violations of the policy, which must include the employee discipline standards for unauthorized access to data contained in section 13.09.	Reviewed the BWC policy and confirmed the current policy does mention disciplinary actions.	In compliance

CANNON FALLS POLICE DEPARTMENT

SECTION 3-18
SUBJECT POLICE BODY WORN CAMERA

INDEX

POLICY

This agency recognizes that Police Body Worn Cameras (BWC) is an effective law enforcement tool. Therefore, the policy of this agency will be to utilize BWC technology in a manner that enhances accountability and transparency for all involved in a police and citizen interaction. This policy does not apply to other police video recording equipment, which is covered by policy 3-5. BWC is only a slice of what was occurring at a given time and is a two dimensional representation of a three dimensional event. The BWC may not record all the information that was seen or heard by those involved in the event and is only one part of the documentation of an event where a full understanding of what occurred is needed.

PURPOSE

The purpose of this policy is to clearly establish for agency personnel the proper use of BWC

technology to achieve the following:

- The primary purpose is to provide evidence collection of events, actions, conditions, and statements made during arrests, critical incidents, and other law enforcement activities.
- To enhance the agency's ability to provide accountability and transparency of officer and citizen interactions.
- To evaluate the performance of officers and to assist in training.

SCOPE

This policy applies to all sworn personnel and those civilian personnel assigned the responsibility of handling digital evidence or information releases.

STANDARDS

3-18.1 DEFINITIONS

Body Worn Camera (BWC) – A camera system that is worn on an individual officer's person that records and stores audio and video data.

Data Subject – The image or voice of any person recorded by a BWC, except of the officer wearing the BWC that captured the data.

Data Transfer – The movement of digital data from a BWC device to the agency digital evidence storage location.

Digital Evidence – Digital data files from PVRE including BV, ICV, BWC or any other agency device capable of capturing audio, video, photographs and stored in a digital format that have an evidentiary value.

Evidentiary Value – Information that may be useful as proof in a criminal prosecution and related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or officer.

General Citizen Contact – A formal or informal encounter between an officer and person(s) that does not have an evidentiary value. Examples including, but not limited to: assisting a motorist with directions, answering general questions or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.

Minnesota Government Data Practices Act (MGDPA) – Refers to Minnesota Statute 13.01, et seq.

Non-general Citizen Contact – Means an officers encounter with a person(s) 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.

Police Video Recording Equipment (PVRE) – Equipment used to record video with or without audio.

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

3-18.2 TRAINING

The agency shall provide all employees responsible for the operation, handling and management of the BWC equipment and data files with training to ensure compliance with this policy.

3-18.3 USAGE

Officers shall only use department approved/issued BWC in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this department.

Officers assigned a patrol shift will utilize a BWC during their work shift. Officers at the beginning of their shift shall determine if the BWC equipment issued to them is working correctly. Problems shall be reported to their immediate supervisor. A BWC not working correctly should be placed out of service and a spare BWC or a BWC from another officer should be utilized. The officer using a different BWC shall create a Miscellaneous Officer Action ICR, and include in the blotter which camera is being used

and the shift the officer is working. Officers should ensure the BWC is worn in one of the approved locations to record events.

A. Approved BWC wear locations:
   1. On the vertical button edge of a uniform shirt or outer jacket.
   2. On a dedicated tab of a uniform shirt or outer jacket.
   3. On a dedicated tab located on outer body armor carrier.
   4. On the pocket of an outer body armor carrier.
   5. Other location submitted in writing based on specific circumstances to the Chief of Police or Designee with a written approval.

3-18.4 ACTIVATION/DEACTIVATION

A. Officers should activate their BWCs when anticipating that they will be 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, non-general 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 must be documented in the ICR and report, if a report is created.

B. Officers have discretion to record any police-citizen encounter regardless if the recording would yield information having evidentiary value, unless such recording is otherwise expressly prohibited.

C. Officers have no affirmative duty to inform people that a BWC is being operated or that they are being recorded.

D. Once activated, the BWC should continue recording until the conclusion of the event, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value or if the event would be recorded by another department PVRE system. 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 circumstances change, officers will reactivate their cameras as required by this policy to capture information having evidentiary value.

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

is acceptable if utilized to comply with section 3-18.5 B, Special Guidelines for Recording, where a temporary blocking would be more appropriate than stopping and starting the BWC.

F. Officers shall not activate the BWC during events where undercover officers are known to be present without prior approval from the undercover officers or supervisor.

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

3-18.5 SPECIAL GUIDELINES OF RECORDING

Officers may, in the exercise of discretion, determine:

1. To use their BWC to take recorded statements from persons believed to be victims and witnesses of crimes, and persons suspected of committing crimes, considering the needs of the investigation and the circumstances pertaining to the victim, witness, or suspect.

2. To use their BWC to record persons being provided medical care if the subject is aggressive towards others or force may be necessary to allow for providing medical care.

3. To use their BWCs when dealing with individuals believed to be experiencing a mental health crisis or event. BWCs shall be activated as necessary to document any use of force, or anticipated need for use of force.

4. If officers respond to a health care facility, mental health care facility, detox, juvenile detention center, or adult detention center for a call of assistance, they may record the event as covered under 3-18.5 A., but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing aggression or a use-of-force incident.

5. Officers should avoid recording law enforcement restricted data on a BWC that may be in a verbal, written or electronic format. Examples including, but not limited to: computer screen or Driver's Licenses, school or medical information.

3-18.6 DOWNLOADING / LABELING RECORDINGS

A. Officers should download the BWC at the end of their shift or when it becomes full. Nothing prevents an officer from downloading more frequently.

B. BWCs will be downloaded in the manner and to location specified during training.

C. Recordings of known evidentiary value or use of force event or an event the officer believes should be retained longer will be labeled and stored as directed during training. These recordings need to be listed in the officer's written report.

D. All other recordings shall be stored designated by agency configuration for downloading. Recording will be labeled as designated during training.

3-18.7 DATA STORAGE MEDIA CONTROL AND MANAGEMENT

A. Data Retention

1. Evidentiary recorded data shall be retained for the period specified in the General Records Retention Schedule for Minnesota Cities. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable retention period.

2. Unintentionally recorded data shall not be retained and will be deleted at the earliest possible time.

3. Non-evidentiary recorded data, or becomes classified as non-evidentiary, shall be retained for a minimum of 90 days following the date of capture.

4. If information comes to light indicating that non-evidentiary data has evidentiary value and it has not been deleted, it will be reclassified as evidentiary data and would be subject to that classifications retention schedule.

5. BWC recorded data that has a value for training purposes; may be reclassified as training data and subject to section 3-18.9. BWC recordings that are retained for training purposes, which no longer have evidentiary value, may be stored outside of the regularly used server. Such recording are still considered department data and may not be disseminated outside the department without prior approval.

B. Digital Data Storage

1. Officers shall only use agency designated digital data storage, as approved by the Chief of Police or designee.
2. The City's Information Technology will determine the best method for backing up the data. If that method is an off-site, cloud based system, they will ensure the data is encrypted and meets the requirements of the Criminal Justice Information Services, Policy 5.4 or successor version.

C. Security/Control of Digital Data

1. Officers shall not intentionally edit, destroy, erase or in any manner alter BWC digital data unless otherwise expressly authorized by the chief or the chief's designee.

2. Upon download from the BWC, digital data will be subject to the same security restrictions and chain of evidence safeguards as any other piece of evidence/property.

3. A copy of any digital data will not be released to a person or agency, other than another criminal justice agency, without prior approval of the Chief of Police or his/her designee.

4. Personally owned devices, including but not limited to computers and mobile devices, shall not be programmed or used to access, view or record BWC digital data, without prior approval from the Chief of Police.

5. Access to BWC digital data from city approved devices shall be managed in accordance with established agency and/or city policy.

6. Agency personnel may access and view stored BWC data 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 BWC recorded data of an incident which they recorded, only for the purpose of preparing a report, giving a statement, or providing testimony about the incident.

7. 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 digital data recorded or maintained by this agency onto public and social media websites.

8. Officers may display portions of BWC data 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 limit these displays, including but not limited to: showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video, to protect against the incidental disclosure of individuals whose identities are not public.

9. Officers shall refer members of the media or public seeking access to BWC recorded data to the responsible authority/data practices designee, who will process the request in accordance with the MGDPA and other governing laws. Employees seeking access to BWC recorded data for non-business reasons may make a request for it in the same manner as any member of the public.

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

3-18.8 DATA RELEASE REQUESTS

Minnesota State Statutes 13.825 classifies BWC recorded data as private data on individuals or nonpublic data. This agency may redact or withhold access to portions of data that are public under this subdivision if those portions of data are clearly offensive

to common sensibilities. BWC data is considered pubic under the following provisions of 13.825:

A. Data that document the discharge of a firearm by a peace officer in the course of duty, if a notice is required under section 626.553, subdivision 2, or the use of force by a peace officer that results in substantial bodily harm, as defined in section 609.02, subdivision 7a.

B. If a subject of the data requests it be made accessible to the public, but subject to redaction if the data contains:

   a. Other data subjects that have not consented to the release.
   b. Data contains images of a peace officer whose identity is protected under section 13.82, subdivision 17, clause (a).

C. Data that are public personnel data under section 13.43, subdivision 2, clause (5).

D. Data made public by an order of the Court.

3-18.9 AGENCY USE OF DATA

The following purposes are approved by the Chief of Police as having a legitimate and specified law enforcement purpose, for the access to the BWC recorded data as provided by Minnesota Statute 13.825, subd 7(b).

A. Supervisors or other personnel as assigned by the Chief of Police or designee 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.

B. Supervisors may randomly review BWC recordings made by officers to ensure the equipment is operating properly and officers are using the devices appropriately in accordance with this policy, and to identify any performance areas in which additional training or guidance is required. Such reviews will be maintained in a log, indicating the purpose of the review.

C. Officers should contact their supervisor to discuss retaining and using BWC recorded data for training purposes. Officer objections to preserving or using certain BWC data for training will be considered on a case-by-case basis.

D. Field training officers may review BWC recorded data, recorded by them or their trainee, with trainees for the purpose of providing coaching and feedback on the trainee's performance.

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

3-18.10 AUDITS

This agency will conduct an annual audit to check for the occurrence of unauthorized access to BWC recorded data. Randomized sampling may be utilized for this process, and statistical results of the audit will be reported to the city council.

This agency will conduct an independent audit on a biennial basis as required by Minnesota Statute 13.825, subd. 9, results of the independent audit will be reported to the city council.

3-18.11 VIOLATION OF POLICY

If an employee misuses the data covered by this policy or intentionally fails to comply with or violates this policy, it will be considered misconduct as covered by section 1-6.07 and such behavior may be grounds for disciplinary action up to and including discharge.

This report was prepared exclusively for the City of Cannon Falls Police Department by Michael Bowe, On-Site Computers Inc. . The findings in this report are impartial and based on information and documentation provided and examined.

Dated: October 7, 2020

On-Site Computers, Inc.

Michael Bowe

Michael Bowe
President
On-Site Computers, Inc.