442.18 Body Worn Camera Pilot Policy

TABLE OF CONTENTS

Contents

INT	TRODUCTION	2
1.	DEFINTIONS	2
2.	OVERVIEW	4
3.	OPERATIONAL OBJECTIVES.	5
4.	ISSUANCE OF BODY-WORN CAMERAS (BWC)	5
5.	REQUIRED BWC USE	6
6.	TESTING	6
7.	MANDATORY, DISCRETIONARY, AND PROHIBTED RECORDING	6
8.	WHEN RECORDING MAY BE STOPPED	8
9.	DUTY TO NOTIFY	9
10.	. FAILURE TO RECORD	10
11.	DATA LABELING	10
	. DOWNLOADING	
13.	. CRITICAL OR SIGNIFICANT INCIDENTS	12
14.	. PRIVATE, CONFIDENTIAL, AND PUBLIC BWC DATA	12
15.	. ACCESS BY DATA SUBJECTS	14
16.	. WATCHING, REVIEWING, AND COPYING BWC DATA	14
17.	. PROTECTION OF BWC DATA / AUDIT	16
18.	. RELEASE TO THE PUBLIC	16
19.	. DOCUMENTING EXISTENCE OF BWC DATA	17
20.	. BWC DATA RETENTION	17
21.	. HANDLING OF EVIDENCE	18
22.	. POLICY COMPLIANCE	18
	. TRAINING	
24.	. BWCs AND THE ICC SYSTEM	19
25.	. DISCOVERY OF POTENTIAL MISCONDUCT	19
26.	. ACCESS TO SENSITIVE PERSONAL RECORDINGS	19

INTRODUCTION

On November 9, 2016, the Saint Paul Police Department will begin a Body Worn Camera (BWC) pilot program in the West District. This general order provides guidelines for use and management of the system, storage and retention of data, and dissemination and review of data captured by devices worn by Saint Paul Police Department personnel during the pilot.

Portions of the policy read as if applicable for the entire department. However the policy applies to, and compliance rests only with, personnel participating in the pilot program. This policy will be evaluated and amended throughout the pilot program.

1. DEFINTIONS

- A. Activate To manually begin recording. There is not an automatic start; officers must manually start the recording process. There is a 30 second video-only buffer.
- B. BWC Body worn camera meeting the definition of portable recording system under Minnesota Statutes section 13.825.
- C. BWC Data Audio or video data collected by a department BWC pursuant to this policy.
- D. BWC Unit Unit to be established, anticipated to include the following roles:

BWC Administrator - sergeant or designee who assigns, tracks, and maintains BWC equipment, oversees needed equipment repairs or replacement, administers user rights and access, and acts as a liaison with the vendor.

BWC Technician - personnel certified or trained in the operational use and repair of BWCs, duplicating methods, storage and retrieval methods and procedures, and who possesses a working knowledge of video forensics and evidentiary procedures.

E. Buffering Mode - When the BWC is on and actively recording video only. In the buffering mode the camera will continuously record video in 30 second loops. Audio is not recorded in the buffering mode.

- F. Label To label BWC Data according to predetermined information classifications.
- G. Critical Incident -
 - Critical Incident for the purposes of this policy includes critical incidents described under General Order 246.09:
 - The officer(s) involved uses deadly force through the discharge of a firearm. Deadly force is defined by Minnesota State Statute 609.066 subd. (1) as any "force which the actor uses with the purpose of causing, or which the actor should reasonably know creates a substantial risk of causing, death or great bodily harm. The intentional discharge of a firearm in the direction of another person, or at a vehicle in which another person is believed to be, constitutes deadly force."
 - Intentional or accidental use of any weapon which results in great bodily harm or death as a result of police involvement.
 - Attempts to affect an arrest or otherwise gain physical control over a person for law enforcement purposes which result in great bodily harm or death.
 - Vehicular incidents related to police actions that result in great bodily harm or death.
 - Critical Incident also includes any incident similar to the examples defined above involving a Saint Paul Police Department employee as determined by the Chief or his or her designee.
- H. Deactivate to stop recording.
- I. Great Bodily Harm Defined by Minnesota Statutes section 609.02, subdivision 8, as bodily injury which creates high probability of death, or which causes serious permanent disfigurement, or which causes a permanent or protracted loss or impairment of

the function of any bodily member or organ or other serious bodily harm.

- J. ICC In Car Camera
- K. MGDPA Minnesota Government Data Practices Act, Minnesota Statutes chapter 13.
- L. META-DATA The date, time, case number, officer's name, and BWC Data label.
- M. Mandatory Recording When the BWC must be activated under this policy if practical and possible without compromising the safety of the officer or public.
- N. Significant Incident includes, but is not limited to, any of the following situations occurring in the line of duty:
 - Critical Incident.
 - Department vehicle accident resulting in substantial bodily harm, great bodily harm, or death.
 - Any incident where the officer's supervisor believes the BWC to be of evidentiary or administrative value.
 - Act of terrorism.
 - Any event that an officer or their supervisor believes should be brought to the immediate attention of department command.
- O. Substantial Bodily Harm Defined by Minnesota Statutes section 609.02, subdivision 7a, as 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.

2. OVERVIEW

This policy sets out guidelines governing the use of BWCs and administration of BWC Data. Compliance with this policy 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.

BWC Data may be used for law enforcement purposes, internal review and use, or public access pursuant to the MGDPA and Minnesota Statutes section 626.8473.

3. OPERATIONAL OBJECTIVES.

Operational objectives include in no particular order of importance:

- A. Assist in resolving complaints against sworn personnel.
- B. Collect evidence for use in criminal investigations and prosecutions.
- C. Deter criminal activity and uncooperative behavior during police encounters.
- D. Document statements and events during the course of an incident.
- E. Enhance officer and public safety.
- F. Enhance officers' ability to document and review statements and actions for internal reporting requirements and for courtroom preparation.
- G. Promote transparency and accountability and build community trust.
- H. Provide additional information for training.
- I. Utilize best practices in the rapidly evolving field of law enforcement.

4. ISSUANCE OF BODY-WORN CAMERAS (BWC)

- A. During the pilot, BWCs will be issued to participating sworn personnel in the Western District who as part of their daily assignment wear the uniform of the day. The pilot will evaluate department-wide deployment for personnel in the following assignments:
 - Patrol
 - K9
 - Traffic/ motors/ mounted

- SWAT
- B. Officers must use the device as trained and may not interfere with the proper functioning of the device.

5. REQUIRED BWC USE

Officers who have been issued a BWC and trained in its use as part of the pilot program are required to wear the BWC as described below:

- A. As part of the uniform when working on-duty (regular or overtime).
- B. When wearing "raid" gear, as applicable.
- C. Officers working in plain clothes or undercover will not be required to wear a BWC during the pilot.
- D. Officers will not be required to wear the BWC when working off-duty during the pilot.
- E. The Chief may designate certain functions (e.g., funeral or ceremony) as exempt from BWC deployment.

6. TESTING

- A. Officers wearing a BWC must test the functioning of the BWC according to the manufacturer's instructions at the beginning of each shift.

 Officers must report any test failure to his or her supervisor.
- B. Officers may not wear a camera that fails the daily test.
- C. If an officer becomes aware of a BWC malfunction during their shift, they should return to fix or exchange the BWC as soon a practically possible.
- D. Officers must document a BWC failure or malfunction according to the manufacturer's instructions for documenting equipment failure.

7. MANDATORY, DISCRETIONARY, AND PROHIBTED RECORDING

A. Mandatory Recording

Understanding that peace officers encounter tense, uncertain, and rapidly evolving situations, to the extent practical without compromising officer safety, officers are required to activate their BWC in preparation for, when initiating, or under the following circumstances and conditions:

- Traffic stops
- Vehicle pursuits
- Arrests
- Frisks
- Searches (e.g., suspect, vehicle, physical area)
- Officer response to resistance or aggression.
- In-custody transports.
- Victim, witness, or suspect interviews except as noted below.
- When ordered by a supervisor for a proper purpose.
- In response to any call or incident where the officer may reasonably expect BWC activation will be required by one of the scenarios listed above.

If activation of the BWC may reasonably be expected, the officer shall activate the BWC as soon as it is practical and safe to do so while responding, and no later than when the officer arrives on scene.

B. Discretionary Recording

This policy does not describe every possible situation where the BWC may be activated. Beyond the mandated scenarios described above, an officer may activate the BWC anytime they believe it should activated based on their training, experience, and judgement, except when recording is prohibited under this policy.

C. Prohibited Recording

 Interactions solely among other employees when not actively investigating or assigned to a call or incident.

- Non-work related activity.
- Within areas of a police facility restricted to personnel-only access, including roll call rooms, locker rooms, break rooms, and report rooms. BWCs should only record citizen contacts inside a police facility if relevant to an investigation or in response to resistance or aggression inside a police facility.
- When interacting with undercover officers or confidential informants, or persons providing information based on confidentiality.
- During a work break.
- At any location where a reasonable expectation of privacy exists, such as a bathroom or locker room, unless responding to or encountering resistance or aggression or necessary for a law enforcement investigation.
- Inside a courtroom during court proceedings unless responding to or encountering resistance or aggression.
- In patient care areas of a hospital, sexual assault treatment center, or other healthcare facility unless responding to resistance or aggression or necessary for a law enforcement investigation.

8. WHEN RECORDING MAY BE STOPPED

Once activated, the BWC must remain on until the incident has concluded; meaning it is reasonable to believe that all arrests are made, arrestees transported, and victim, witness, and suspect interviews are completed unless:

- A. The incident or event is of such duration that the BWC is stopped to conserve power or storage capacity.
- B. The officer reasonably believes deactivation will not result in the loss of important documentary information.
- C. Deactivation is reasonable and necessary to protect the safety of the officers or others.

- D. Deactivation is approved or ordered by a supervisor.
- E. Deactivation is necessary to protect the identity of a person or other data entitled to protection under the MGDPA.
- F. Upon request by a victim or witness, provided the request does not conflict with (B) or (C) above. The officer should consider the totality of the circumstances before deactivating a BWC and determine the best approach for a particular circumstance. For example, deactivation may be the best option if a BWC inhibits a victim or witness from providing information. Deactivation must be documented in an incident report, or if no incident report in CAD comments.
- G. Recording may be temporarily paused or muted, depending on technology capability, to exchange information with other law enforcement officers or those working in official capacities as part of a law enforcement investigation (e.g., medics, firefighters, medical examiners, dispatchers, civilian employees of government agencies, etc.). An officer must note their intent to pause and resume recording either verbally on the BWC or in an incident report, or if no incident report in CAD comments.
- H. BWCs may be deactivated during non-enforcement activities, such as waiting for a tow truck or a family member to arrive or protecting accident scenes. Nothing in this section is intended to discourage an officer from recording during non-enforcement situations when in his or her judgement the recording may be beneficial.
- I. An officer's decision to stop, pause, or mute recording in a situation in that would otherwise be recorded under this policy must be noted verbally (unless safety or other circumstances make the verbal notation unsafe or unreasonable) on the camera before stopping or pausing. The decision to stop recording and reasons for the decision must also be noted in an incident report, or if no incident report in CAD comments.

9. DUTY TO NOTIFY

Minnesota is a "one-party consent" state, which means that only one party to a communication needs to consent for a recording, unless the recording is made for the purpose of committing a criminal or tortious act. Minn. Stat. § 626A.02, subd. 2. Therefore, officers are not required to notify citizens when recording. However, if reasonable and consistent with the officer's safe and efficient

performance of duties, the officer should confirm whether the incident is being recorded on a BWC if asked.

10. FAILURE TO RECORD

If an officer is unable or fails to activate his or her BWC in one of the mandated scenarios described in this policy, the BWC must be activated as soon as it is safe and practical to do so. Officer and public safety is the highest priority. Facts surrounding the failure to record must be documented in an incident report, or if no incident report in CAD comments.

Note that officers involved in a critical incident do not complete reports. Any requirements of this section for officers involved in a critical incident will be fulfilled by the report of an investigator.

11. DATA LABELING

- A. Officers must label BWC Data files at the time of video capture or transfer to storage, and should contact a supervisor with questions about appropriate labeling. Officers should assign as many of the following labels as are applicable to each file:
 - 1. **Evidence criminal:** The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision. Includes arrest, citation issued, or report prepared for charging.
 - 2. Evidence investigation of a death.
 - 3. **Response to resistance or aggression:** The event involved the application of force by a law enforcement officer. For the purposes of labeling and retention, includes discharge of a firearm.
 - 4. **Administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer.
 - 5. **Civil other:** The recording has potential evidentiary value for reasons identified by the officer at the time of labeling. For the purposes of labeling and retention, includes property damage and accidents.

- 6. **General Citizen Contact**: Recordings of general citizen contacts that do not contain evidence.
- 7. **Extraneous Recording:** The recording does not contain any of the foregoing categories of information and has no apparent value to the city, public, police department, or any other party. Includes equipment maintenance.
- B. During the pilot, the department will evaluate options to allow flagging of protected data in Meta-Data, including:
 - Victims and alleged victims of criminal sexual conduct and sex trafficking
 - 2. Victims of child abuse or neglect
 - 3. Vulnerable adults who are victims of maltreatment
 - 4. Undercover officers
 - 5. Informants
 - 6. Victims of and witnesses to crimes, if the victim or witness has requested not to be identified publicly
 - 7. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system
 - 8. Mandated reporters
 - 9. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness
 - 10. Juveniles who are or may be delinquent or engaged in criminal acts
 - 11. Individuals who make complaints about violations with respect to the use of real property
 - 12. Other individuals whose identities the officer believes may be legally protected from public disclosure, including when the video is clearly offensive to common sensitivities.

12. DOWNLOADING

During the pilot project, officers are required to download the BWC Data according to the instructions and training of each respective vendor under evaluation.

13. CRITICAL OR SIGNIFICANT INCIDENTS

In the event of a Critical or Significant Incident, all officers who are involved or who witness the incident must turn off their BWCs when instructed by a supervisor or investigator assigned to the incident. It is the responsibility of a scene supervisor to ensure compliance with this section.

All involved or responding officers must maintain custody of their BWC equipment until the forensic services unit or crime lab of the investigating agency takes custody of the equipment. In the event that an officer will be photographed as part of the investigation, the officer should leave their uniform intact, including BWC equipment, until photographs are completed. Authorized crime lab personnel will be responsible for ensuring that all video is properly downloaded. Once all downloads are completed, BWC equipment will be returned to the officer or their supervisor unless the device itself is evidence, in addition to any BWC Data created by the device. If the BWC device is evidence it must be handled in the same manner as any other evidence.

In the event a crime lab does not respond to a Significant Incident, the supervisor must ensure BWC Data is properly downloaded before returning the BWC to the officer.

14. PRIVATE, CONFIDENTIAL, AND PUBLIC BWC DATA

All BWC Data is the property of the SPPD and is government data subject to the laws of the State of Minnesota.

When access to BWC Data is authorized by applicable law, the SPPD will provide the person accessing the data a copy of the department's video/audio advisory. This advisory is not required to be given to other law enforcement or government employees accessing data as part of a criminal investigation.

To prevent damage to, or alteration of, the original BWC Data, it may not be copied, viewed, or inserted into any device not approved by the department

BWC Technician or technology/FSU staff. When reasonably possible, a copy of the BWC Data must be used for viewing in order to preserve the original data (unless otherwise directed by a court).

Minnesota Statutes section 13.825, subdivision 2, defines BWC Data as presumptively *private* about the data subjects unless there is a specific law that makes the BWC Data *confidential* or *public*.

Data subjects are defined as:

- Any person or entity whose image or voice is documented in the data.
- The officer who collected the data.
- 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.

Confidential BWC Data is data that is collected or created as part of an active criminal investigation. This takes precedence over private and public classifications listed below and allows an agency to withhold release of data while an investigation is active.

Public BWC Data is:

- Data documenting the discharge of a firearm by an officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.
- Data that documents the use of force by an officer resulting in substantial bodily harm.
- Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than an officer) who has not consented to the public release must be redacted. In addition, data on undercover officers must be redacted.
- Data that documents the final disposition of a disciplinary action against a public employee.
- If another provision of the MGDPA classifies data as private or otherwise not public, that data retains the MGDPA classification.

15. ACCESS BY DATA SUBJECTS

As required by statute, an individual must be allowed to access BWC Data about him- or herself and other data subjects in the recording, but access will not be granted to data:

- Collected or created as part of an active investigation.
- Restricted by law from disclosure to the person seeking access, such as portions that would reveal identities protected by Minnesota Statutes section 13.82, subdivision 17.

Unless the data is part of an active investigation, an individual data subject must be provided with a copy of the recording redacted as follows:

- Data on other individuals in the recording who do not consent to the release must be redacted.
- Data that would identify undercover officers must be redacted.
- Data on other officers who are not undercover, and who are on duty and engaged in the performance of official duties, will not be redacted.

16. WATCHING, REVIEWING, AND COPYING BWC DATA

Officers are authorized to access not public (confidential or private) BWC Data for any legitimate law enforcement purpose, including but not limited to report writing. Nothing in this policy restricts an officer from reviewing BWC Data created by the BWC issued to and operated by the officer, excepting department policy 235.20 Administrative Lockdown.

- A. Officers involved in a Critical Incident may view or listen to BWC Data of the incident only after:
 - The officer has met with the Saint Paul Police Federation representative or legal counsel, if requested, and
 - The officer and legal counsel have met with the investigative entity or designee regarding the process for a Critical Incident set out in General Order 246.09: Investigations-Incidents Where Serious Injury or Death Result During Police Custody or Involvement.

- B. An investigator assigned to a related criminal investigation may review BWC Data relevant to their investigation.
- C. BWC Data relating to a criminal matter will be disclosed to the appropriate prosecuting authority.
- D. BWC Data may be further disclosed to court personnel as authorized by applicable rules of procedure and Minnesota Statutes sections 13.03, subdivision 6, and 13.825, subdivision 2 (d).
- E. Officers who become aware of BWC Data that may contain training value should notify their supervisor. BWC Data may be shown for staff or public safety training purposes with the consent of all data subjects. If an employee objects to this use, the objection must be submitted to the training unit commander. Training unit staff will review the objection to determine if the training value outweighs the objection. The training unit will submit a recommendation to the Chief of Police for final determination. Field training officers may utilize BWC Data with trainees for the purpose of providing coaching and feedback on the trainee's performance.
- F. Nothing in this policy limits or prohibits the use of BWC Data by the department to evaluate alleged misconduct or as a basis for discipline.
- G. Copies of BWC Data must be requested through the technology unit during the pilot program. Officers may not copy or record BWC Data with smart phones, video cameras, or any other means.
- H. Supervisors may not access or review BWC Data for the purpose of surveillance of any employee. However, BWC Data may be accessed by internal affairs or a supervisor investigating a complaint of misconduct. A complaint of misconduct may include any allegation of improper procedure or misconduct, from an informal allegation or question to a formalized internal affairs complaint.
- I. Officers needing to access BWC Data from another officer's BWC must submit in writing a request to their supervisor to access data from another officer's BWC. Requests may be granted only for a legitimate purpose relating to employment, such as the need to complete a report.
- J. Response to Resistance or Aggression Review
 - BWC Data may be accessed as part of the department's review of officer

response to resistance or aggression. Only supervisors and department personnel who have the responsibility to review a response to resistance or aggression may access BWC Data pertaining to the incident.

K. Pursuit Review

BWC Data showing a vehicle pursuit may be accessed by supervisors and department personnel who have the responsible to review the incident. BWC Data showing an accident may be disclosed to the Accident Review Board pursuant to General Order 640.07.

L. Showing BWC Data to Witnesses

Officers may display portions of BWC Data to witnesses as necessary for purposes of investigation as allowed by Minnesota Statutes section 13.82, subdivision 15, which states this is allowable to "aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest."

17. PROTECTION OF BWC DATA / AUDIT

The SPPD will protect BWC Data in compliance with state law and this policy. To that end, the department will:

- A. Restrict access to BWC Data according to an authorized employee's access credentials, and
- B. Maintain an electronic notation of the date, time, and person with regard to each access to data. During the pilot, all employees who access not public BWC Data will be required to document the reason for their access according to system capabilities.

18. RELEASE TO THE PUBLIC

- A. During the pilot, only technology unit or forensic media staff will be authorized to make copies of BWC Data, on any device or in any media. The original copy of the data will be stored according to the retention schedule in this policy.
- B. Copies made by the BWC technician or department forensic media staff must be for lawful purposes including but not limited to data requests

- under the MGDPA, department purposes, criminal litigation, and civil litigation.
- C. When possible, the department will notify the officer whose device created the data before BWC Data are released to the public.

19. DOCUMENTING EXISTENCE OF BWC DATA

- A. If a BWC was activated during any call or incident, whether at the scene or perimeter, the wearing officer must inform dispatch of their presence so they will be assigned to the incident in the computer aided dispatch system.
- B. Officers must document whether BWC Data was created in the applicable incident report, or if no incident report in CAD comments.

20. BWC DATA RETENTION

All BWC Data will be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data. During the pilot, the following additional retention periods apply:

Label	Retention Period	Section or General Records Retention Schedule for Minnesota Cities Code
Evidence - Criminal	Expiration of all appeal periods or corresponding statute of limitations, whichever is later	POL 05840, 05900
Investigation of a Death	No expiration	POL 05870
Response to Resistance or Aggression	6 years	Minn. Stat. § 13.825, POL 05920
Administrative / Internal Investigation	6 years	Minn. Stat. § 13.825, POL 05880
Civil - other (includes property damage and accidents)	6 years	Minn. Stat. § 13.825
General Citizen	1 year	Minn. Stat. §

Contact		13.825, POL 05860
Extraneous Recording	90 days	Minn. Stat. § 13.825, POL 05830

BWC Data will be retained in accordance with the MGDPA, General Retention Schedule for Minnesota Cities, Ramsey County Evidence Retention Policy, court order, or applicable statute of limitations or preservation period.

Upon written request by a BWC Data subject, the department will retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. The department will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received.

The duration of any BWC Data evidence retention may be increased as needed.

21. HANDLING OF EVIDENCE

- A. BWC Data will be handled as evidence.
- B. When a BWC is used to collect data in serious injury/fatal crash investigations, the original recording will be maintained as part of the complete crash investigation file in the forensic services unit and not as part of the crash file at citywide services. Recordings that are potentially subject to continuing judicial review will be retained by the department according to the applicable retention period.
- C. Evidence containing data that must be retained as part of pending civil action or are collected as part of an active investigation will be retained by the department according to the applicable retention policy, statute of limitations, or evidence preservation period.
- D. When BWC Data contains evidence for a case that is being investigated by another agency, that agency will be provided a duplicate copy of the recording for a specified law enforcement purpose with the written approval of the Chief of Police or his or her designee.

22. POLICY COMPLIANCE

Supervisors shall monitor compliance with this policy. The unauthorized access to or disclosure of BWC Data may constitute misconduct and subject individuals

to disciplinary and criminal penalties pursuant to Minnesota Statutes section 13.09.

23. TRAINING

Employees must complete the BWC training program before using a BWC to be developed during the pilot program.

24. BWCs AND THE ICC SYSTEM

BWCs do not replace the ICC system. This policy does not replace the ICC policy. ICC continues to be governed by General Order 442.17 In-Car Camera Policy. However, officers wearing a BWC are exempt from the wireless microphone portion of the ICC policy.

25. DISCOVERY OF POTENTIAL MISCONDUCT

Any employee reviewing BWC Data for any reason should focus on the incident in question and may only access data necessary and relevant to their authorized reason for access.

If an employee reviewing BWC Data suspects a policy violation they should report the violation to their supervisor.

26. ACCESS TO SENSITIVE PERSONAL RECORDINGS

In the event of unintentional or inadvertent BWC recording, such as a personal conversation that captures sensitive personal information for which access should be restricted, an officer may submit a written request to his or her commanding officer to restrict access to that portion of BWC Data.