

# National Institutes of Health

# **Division of Police**

M NEW L	I AMENDS 🗆 I	RESCINDS.
By Autho	ority of the Ch	nief of Police
Chief C	Cleveland L.	Spruill Sr.

# Directive 463 - Body Worn Cameras

<b>Effective Date:</b>		Cancels:	
<b>Updated Date:</b>	Section(s):		<b>Review Date:</b>
<b>Updated Date:</b>	Section(s):		
<b>Updated Date:</b>	Section(s):		
CALEA	41.3.8.a, 41.3.8.b, 41.3.8.d, 4	11.3.8.e, 41.3.8.f, 41.3.8.g	

### **CONTENTS**

- 2.8.01 PURPOSE/POLICY
- 2.8.02 **DEFINITIONS**
- 2.8.03 EQUIPMENT CONSIDERATIONS
- 2.8.04 STORAGE AND ACCESS TO DEVICES
- 2.8.05 OPERATIONAL MODES
- 2.8.06 DEVICE FEATURES
- 2.8.07 RECORDING PROCEDURES
- 2.8.08 EXEMPTIONS, PROHIBITIONS
- 2.8.09 SPECIAL LOCATIONS ACCESS
- 2.8.10 TO BWC FILES CRITICAL
- **2.8.11 INCIDENTS**
- 2.8.12 SUPERVISOR RESPONSIBILITIES
- 2.8.13 BWC SECTION RESPONSIBILITIES
- 2.8.14 COURT PROCEDURES PROVISIONS
- 2.8.15 OF BWC FILES CLASSIFICATION,
- 2.8.16 RETENTION AND DOCUMENTATION
- 2.8.17 FREEDOM OF INFORMATION ACT

# 2.8.01 PURPOSE/POLICY

[41.3.8a]

- 1. The purpose of this policy is to establish comprehensive procedures for the management of the National Institutes of Health (NIH) Division of Police (DP) Body-Worn Camera (BWC) program, including guidelines for the appropriate use, maintenance, and storage of BWCs, protocols for accessing and sharing BWC footage, and measures for ensuring transparency and accountability in law enforcement activities.
- 2. BWC equipment will be provided to sworn Division of Police (DP) employees. All BWC-captured images, video, audio, and data are the property of the National Institutes of Health Division of Police.
- 3. DP Employees shall use BWCs and associated software, hardware, and equipment according to this policy to optimize documentation, meet operational goals, and maintain program and evidence integrity.

- 4. Implementing a BWC program is crucial to enhancing trust, professionalism, transparency, and procedural justice in police-community encounters. The program is anticipated to bring several benefits, including strengthened accountability, improved officer safety, efficient investigations, effective evidence collection, thorough court preparation, successful criminal prosecution, enhanced training, and accurate resolution of complaints against Division of Police (DP) employees. [41.3.8a]
- 5. BWC technology should never replace an individual's reasonable beliefs and perceptions during an incident, nor should it discount the physiological response that may occur during critical situations.
- 6. BWC recordings should not be relied upon as the sole source of truth, as they only capture video and audio evidence from the camera's physical position and may not reflect the full perspective of the officer.
- 7. BWC files should be considered as one element in understanding an incident and should be combined with the officer's experience, perceptions, state of mind, and processing of senses to form a more comprehensive understanding. BWC technology only captures a limited and less detailed image compared to the human senses, and an officer's experience and recollection may differ from what is recorded.
- 8. The safety of all individuals involved should always be the top priority, and recording events should not interfere with this.

  [41.3.8a]

# 2.8.02 DEFINITIONS

- 1. Activation: The start of a BWC recording that captures audio and video evidence.
- 2. <u>Audit Trail</u>: An electronic tracking system that records uploads, views, downloads, transfers, and tracks modifications to copies of BWC files.
- 3. <u>Body-Worn Camera (BWC)</u>: Wearable recording device that captures audio and video of an incident or encounter from an officer's perspective.
- 4. BWC File: A recording of video and audio evidence captured from a BWC device.
- 5. <u>Buffering Mode</u>: An operational mode that facilitates continuous recording, but only saves the recording to permanent storage when the officer manually activates the recording or when a signal event occurs.
- 6. <u>Critical Incidents</u>: Incidents involving police use of lethal force, in-custody deaths, or other actions resulting in death or serious bodily injury.
- 7. <u>Deactivation</u>: The termination of a BWC recording.
- 8. <u>Docking Station</u>: A hardware device that charges, updates firmware, and uploads BWC files.
- 9. Event Mode: An operational mode where the BWC is actively recording both audio and video.
- 10. Metadata: Searchable data specific to the digital file used to identify digital evidence

and required to be added to BWC files.

- 11. <u>Mute Mode</u>: An operational mode where the audio BWC's audio recording feature is disabled, but the camera continues to record video footage.
- 12. <u>Plainclothes Officer</u>: Sworn employees not wearing a department-issued uniform and displaying limited to no law enforcement markings or insignia.
- 13. <u>Signal Technology</u>: Technology that automatically activates BWC recordings when a firearm is removed from a holster.
- 14. <u>Sleep Mode</u>: An operational mode where the BWC is placed in an idle state that disables recording and buffering.
- 15. <u>Stealth Mode</u>: An operational mode where the BWC disables LED lights, sounds, and vibrations.

## 2.8.03 EQUIPMENT CONSIDERATIONS

# A. USE, CARE, AND MAINTENANCE

- 1. All sworn employees of the DP will be assigned a BWC device and associated hardware and software.
- 2. Employees shall not alter, dismantle, or tamper with any hardware or software component of the BWC program. The use of BWC files shall not be discriminatory, arbitrary, or capricious.
- 3. Employees shall use, care, maintain their BWC hardware and software consistent with DP training and manufacturer instructions.
- 4. Only authorized employees who have completed DP training may operate BWC hardware and software. Training for employees will cover policy, procedures, and best practices for operating the BWC system to ensure that it is used consistent with this policy. The training will also include hands-on practice using the hardware and software and instruction on how to properly store, handle, and secure BWC files.
- 5. Employees shall monitor their BWC device's battery level during their duty tour recharging or switching to an alternate battery if needed.

### **B. WEAR AND PLACEMENT**

- 1. Employees will be issued numerous BWC mounts designed to accommodate varying uniforms, equipment, and individual preferences. Only mounts issued by the DP may be utilized.
- 2. Employees shall mount their BWC on their person and in a location that allows for effective recordings. Supervisors may instruct relocations if necessary.
- 3. BWC devices shall be mounted on the outermost garment, or in a way that does not

unreasonably interfere with the device's audio and video function.

- 4. All employees wearing Class B or C uniforms must position their BWC device in front of their body, with the device facing forward and centered or slightly off-center. The device should be located no lower than the navel line and below the height of the shoulders. Officers will be exempt from wearing or using BWC while in Class A Uniforms or while they are engaged in specialized or non-operational functions, provided they have the prior written approval of the Chief of Police or his designee.
- 5. Plainclothes employees shall position their BWC device with the device lens facing forward, centered or slightly off-center. The device should be worn at or above the beltline and no higher than shoulder height.
- 6. It is prohibited to intentionally obstruct, shield, or interfere with the device's audio or video functions.

## C. PRE-SHIFT INSPECTION

- 1. At the beginning of their shift, employees shall inspect their assigned BWC devices to ensure that they are in good working order. Any malfunctioning equipment shall be returned to a Body-Worn Camera Coordinator as soon as practical.
- 2. If an employee does not have a functioning BWC device for use while on duty or during an off-duty detail, they shall inform a supervisor. The supervisor will decide the appropriate course of action, to include the option to provide the employee with a loaner device.

  [41.3.8e]
- 3. Use of loaner devices may only be done with the approval of a supervisor.

## D. END OF SHIFT RESPONSIBILITIES

- 1. BWC devices shall be docked before an employee concludes their shift. Employees may request assistance from a coworker to complete this task.
- 2. Before completing their shift, employees shall input the required metadata for each recording. It is strictly prohibited to carelessly or intentionally miscategorized metadata.

# 2.8.04 STORAGE AND ACCESS TO DEVICES

- 1. All BWC files are stored within a cloud-based digital evidence management system that is designed to securely store, manage, and share digital evidence such as videos, images, and audio recordings.
- 2. While on duty, employees shall have ready access to their assigned BWC devices.
- 3. Off-duty employees operating take-home vehicles shall have access to their BWC device while operating the vehicle.
- 4. Off-duty employees assigned take-home vehicles shall ensure they can promptly retrieve their BWC if called back to work. It is recommended that employees store their BWCs in a secure location alongside their other law enforcement equipment.

- 5. Employees are responsible for securing their BWC devices when not in use. BWCs will not be stored in an unattended vehicle for an extended period while off-duty and will not be left in the passengers' compartment of vehicles equipped with a trunk.
- 6. When not in use, employees shall ensure that all assigned BWC devices are fully charged (90% or higher) or in the process of becoming fully charged by using a docking station or portable charger.

# 2.8.05 OPERATIONAL MODES

- 1. All employees shall wear and operate their assigned BWC device consistent with this policy.
- 2. The BWC device is equipped with multiple operational modes, and employees are required to comply with this policy when using any of these modes.
- 3. The following subsections are the various BWC operational modes Buffering, Event, Sleep, Mute, and Stealth Mode and their required application.

### A. BUFFERING MODE

- 1. Buffering Mode is the default operational mode for the BWC, and employees shall keep their device in this mode while performing official duties unless otherwise approved by this policy.
- 2. While buffering, the BWC device captures new video (without audio) and concurrently overwrites old video as time passes. This record/overwrite process features Pre-Event recording, allowing devices to capture the moments leading up to device activation.
- 3. Buffered video is not permanently stored and will be overwritten eventually, except if a BWC device is activated. In that case, 60 seconds of video (without audio) that occurred before activation will be attached to the BWC file.

### **B. EVENT MODE**

- 1. Event Mode is when the BWC device is activated for recording, and it will capture a video/audio recording until the user deactivates the recording. Additionally, 60 seconds of buffered video (without audio) captured before the event will also be recorded.
- 2. Event Mode can be initiated by manual activation by the user or signal activation following the removal of a firearm from its holster.
- 3. To determine when to activate a BWC device in Event Mode, employees shall refer to the guidelines provided in policy 2.8.07A Device Activation.

# C. SLEEP MODE

1. Sleep Mode is designed to provide employees with temporary privacy during personal and/or protected activities. When in this mode, the BWC device is in an idle state that disables recording, buffering, and pre-event recording.

- 2. Employees are required to place their BWC device in Sleep Mode when entering restrooms, locker rooms, dressing rooms, NIH Facilities, Clinical Centers, Hospitals, other patient care facilities or laboratories unless an incident or circumstance requires a recording. Additionally, when performing or witnessing a strip search, employees shall activate Sleep Mode. Upon exiting these locations, the device shall be returned to either Buffering Mode or Event Mode if a recording is required.
- 3. Sleep Mode shall not be used for any other purpose than the specified ones mentioned above, unless authorized by a supervisor.

### D. MUTE MODE

- 1. Mute Mode is intended to disable audio recording while a BWC device is actively recording video.
- 2. NIH understands that employees may need to engage in personal, sensitive, or confidential conversations while using their BWC device. To accommodate these conversations, employees may activate Mute Mode at their discretion when the following conditions are met:
  - i. The employee is not in the immediate presence of a community member directly involved in the incident.
  - ii. The employee needs to engage in a conversation related to job-related training, coaching, counseling, operational tactics and investigative opinions/theories, or conversations of a more personal nature with a spouse, family member, labor organization representative, medical professional, legal counsel, spiritual advisor, or any other similarly purposed conversation.
  - iii. Before activating the Mute Mode function, employees shall verbally state the reason for muting, such as "personal conversation," "training discussion," or "conversation with a supervisor." The device should be unmuted as soon as possible and before undertaking any operational action or engaging/re-engaging with parties involved in an incident, when practical.
- 3. By permitting Mute Mode, NIH recognizes the importance of employee privacy and confidentiality in sensitive conversations, while maintaining video capture for transparency and accountability purposes. This policy embodies our commitment to striking a balance between safeguarding employee privacy rights and ensuring transparency and accountability in all interactions.

### E. STEALTH MODE

- 1. Stealth Mode is designed to disable LED lights, sounds, prompts, and vibrations on the BWC device. In the interest of officer safety, employees may use their discretion to activate Stealth Mode.
- 2. Stealth Mode does not impact the BWC device's ability to capture and record audio and video.

## F. POWERED-OFF MODE

- 1. Powered-Off Mode occurs when the BWC device is turned off, and all camera functions/operations are disabled.
- 2. Employees may use this mode when they are off-duty or inside NIH Facilities.

## 2.8.06 SPECIAL FEATURES

### A. SIGNAL ACTIVATION

- 1. BWC devices are equipped with Signal technology, which enables the device to automatically transition from Buffering Mode to Event Mode when activated.
- 2. Signal technology is designed to activate any BWC device within a 40-foot range when a duty firearm is removed from a technology-equipped holster.
- 3. Although Signal technology is a valuable tool, it is susceptible to malfunctions and therefore cannot be relied upon as the sole means of activating a BWC. To ensure accountability and transparency, employees are required to manually activate their BWCs whenever it is safe and practical to do so. This redundant activation serves as a contingency plan in case of Signal technology failures, ensuring that critical moments are still captured on video.
- 4. Employees are not permitted to disable or interfere with Signal technology and shall promptly report any issues or malfunctions to a supervisor.

## **B. GPS MAPPING**

- 1. BWC devices have GPS mapping capability in Buffering Mode and/or Event Mode.
- 2. GPS mapping is restricted to sworn supervisors for operational purposes, such as matters related to officer safety, supporting tactical operations, and strategic initiatives related to large-scale incidents or special events.

## C. LIVE STREAMING

- 1. BWC devices are equipped with a Live Streaming feature that enables authorized users to remotely access a live video feed. To ensure security and privacy, the Live Streaming feature can only be activated when the device is actively recording, and remote viewers are unable to remotely activate the device.
- 2. Access to the Live Stream feature is restricted to supervisors only and shall be utilized solely for operational purposes related to officer safety and tactical objectives. This includes monitoring pursuits, high-risk traffic stops, confrontations with armed, violent, or resistant suspects, building searches, officer location efforts, injured officer assistance, or when authorized by the user.
- 3. When a Live Stream feature is activated on a device, the device operator will be notified

through a unique audio, haptic, purple LED, and icon display.

4. Live Streaming is not intended as a substitute for in-person response or supervision and should only be employed as a supplementary tool, considering the totality of circumstances.

## D. PRE-EVENT RECORDING

- 1. BWCs have Pre-Event recording capabilities to capture events leading up to activation due to the unpredictable nature of law enforcement.
- 2. Pre-Event recording captures only video (no audio) of the preceding 60 seconds leading up to BWC activation.

# 2.8.07 RECORDING PROCEDURES

### A. DEVICE ACTIVATION

[41.3.8b]

- 1. While there are many situations that require BWC activation, employees must rely on their best judgment to determine when to activate the device in situations not explicitly covered by this policy.
- 2. Employees shall activate their BWC device before the activity to be recorded or at the earliest safe and practical opportunity.
- 3. To ensure complete and accurate records of official law enforcement contacts and activities, employees are required to activate their BWCs in the following circumstances:
  - a. In-person interactions with members of the public, unless such contact is informal, non-investigative, and non-adversarial. Examples of public interactions that require BWC activation include, but are not limited to, arrests, detentions, consensual encounters intended to be investigative in nature, interactions with adversarial individuals, contact with mental health consumers needing services, traffic stops, and interviews with suspects, victims, and witnesses. Examples of public interactions that do not require BWC activation include, but are not limited to, non-enforcement and non-investigative activities such as community engagement, informal conversations, non-adversarial discussions, information sharing, and community meetings.
  - b. Application of force, the threat of force, or where force is reasonably anticipated.
  - c. Use of law enforcement weapons, such as firearms, pepper spray, or impact weapons.
  - d. On-scene activities related to an active search, pursuit, or apprehension of a fleeing, concealed, or barricaded individual.
  - e. On-scene activities associated with the care and investigation of an injured or deceased individual.
  - f. On-scene searches of individuals and tangible property, as well as any subsequent seizures of property or evidence, excluding those searches occurring within NIH Facilities.

- g. Activities within the boundaries of a crime scene.
- h. Emergency vehicle operations, including vehicle escorts where emergency equipment is continuously or intermittently activated.
- i. Transporting members of the public, whether in custody or not, except during a department-approved ride-along.
- j. Immediately following any officer-involved accident, injury, or vehicle crash, unless it is impractical or unsafe to do so.
- k. Obtaining a breath or blood sample for a DUI arrest, including during the observation period.
- 1. As directed by a supervisor.
- 4. Employees may record incidents that are not explicitly covered by this policy if it serves a law enforcement purpose and is not otherwise restricted by policy.

## B. DEVICE DEACTIVATION

[41.3.8b]

- 1. Once a BWC is activated, it shall continue to record without disruption until the incident/event concludes. An incident may be considered concluded once the activities requiring BWC activation have ceased and are not expected to resume for the duration of the incident.
- 2. Before deactivating the BWC, employees shall briefly state the rationale for deactivation (e.g., "Deactivating because the incident has transitioned to an investigative phase").
- 3. Employees are expected to exercise sound judgment when deactivating their BWCs and should prioritize recording in situations where there is uncertainty or ambiguity regarding whether deactivation is appropriate. Appropriate deactivation instances may include but are not necessarily limited to:
  - a. after interviewing a crime witness and proceeding to document the investigation in a police report.
  - b. after departing an incident scene and terminating future involvement; after concluding a traffic stop and the violator has left the scene.
  - c. after gathering crime evidence and returning to NIH Facilities to process the evidence.
- 4. Employees shall remain vigilant, as static situations can evolve rapidly, potentially necessitating unanticipated BWC reactivation. If circumstances change or additional recording is needed, employees must reactivate their BWCs immediately, or as soon as it is safe and practical to do so.
- 5. In exceptional cases not explicitly addressed by the policy, supervisors may permit employees to deactivate their BWCs. Such approvals should be assessed on an individual basis, with supervisors thoroughly considering the department's and community's interests before making a decision.

### C. DELAYS AND FAILURES TO RECORD

- 1. Any failures to record or material delays in recording shall be reported to a supervisor as soon as possible. The supervisor will consider the circumstances and take appropriate action consistent with DP policies.
- 2. Employees are required to document any instances of failure to record or material delays in recording related to police reports. If a report is not completed, the employee should provide documentation via email to their immediate supervisor.

# D. ACCIDENTAL RECORDINGS

- 1. If a BWC is accidentally activated and the resulting recording serves no law enforcement or administrative purpose, employees may submit a deletion request to their immediate supervisor for approval. The request should include sufficient information (*e.g.*, *date*, *time*, *CAD number*) to locate the recording, along with a brief narrative explaining the reason for deletion. The supervisor shall forward the request to a BWC Coordinator without reviewing the BWC file.
- 2. Upon receiving a deletion request, the BWC Coordinator will evaluate the associated BWC file to ascertain if it holds any official law enforcement or administrative value. If the recording is deemed purposeless, the BWC Section will proceed with its deletion and document the action in an audit log.
- 3. If an employee is uncomfortable with their BWC file being reviewed by a BWC Coordinator due to personally sensitive images, they may request an alternative method to protect their privacy. The request should include the employee's privacy concerns and a general description of the file's contents (e.g., "device inadvertently activated while inside a locker room"). In such cases, the file may be transferred to a confidential, secure storage location inaccessible without approval from the BWC Coordinator. However, it is important to note that the recording will still be retained for the longest retention period and may be subject to examination if it is later alleged or determined to be relevant to a law enforcement or administrative purpose.

# E. PRIVACY AND PUBLIC NOTICE CONSIDERATIONS

- 1. While on NIH campuses, employees are not required to obtain consent or provide notification to members of the public when recording an interaction. However, employees should remain mindful that choosing to provide notification may be beneficial in deescalating incidents and achieving compliance. While off campus in the states of Maryland and Montana, notice should be provided to members of the public when recording an interaction.
- 2. Employees shall answer affirmatively if asked if an interaction is being recorded, unless doing so would adversely impact officer safety or an investigative objective.
- 3. Employees are not required to deactivate their BWC at the request or demand from a member of the public. However, employees may choose to honor the request if they believe it will improve the outcome of the interaction. Employees who choose to comply with a request to deactivate their BWC shall comply with all the following conditions:

- i. The decision to deactivate the BWC device shall be based on the best judgment of the employees and the desired outcome of the law enforcement interaction.
- ii. The request for deactivation shall be initiated by a member of the public, and employees shall capture the request on their recording and document it in a report.
- iii. The interaction shall be non-confrontational and stable, with no foreseeable need for force or apprehension.
- iv. Employees shall be accompanied by at least one other employee who can serve as a witness.
- 4. Supervisors have the authority to permit employees to deactivate their BWCs in situations that do not meet the above conditions, based on their best judgment and consideration of DP and community interests.
- 5. Employees shall reactivate their BWC as soon as practical if the conditions listed above are no longer being met or if the situation changes in a way that requires BWC activation.

## F. REPORTING PROCEDURES

- 1. Employees are required to indicate in their police reports whether a BWC was activated during a reportable incident. Officers are required to indicate the reason for not recording the incident.
- 2. Employees need to be cognizant of the distinctions between their personal observations and the information gathered after watching a BWC file, taking care not to conflate the two. Employees shall clearly document the source of their information when reporting.

# 2.8.08 EXEMPTIONS AND PROHIBITIONS

## A. EXEMPTED EMPLOYEES

- 1. Certain employees are exempt from the BWC wear and use requirement, fully or in part, based on the nature of their assignment. These exemptions are as follows:
  - a. <u>Undercover Employees</u>: Employees assigned to full-time undercover assignments are not required to wear and use their BWC during investigative or administrative tasks. However, when transitioning to an enforcement role, and if time and circumstances permit, they shall wear and use their BWC in accordance with this policy. For these employees, it is advised to attach the BWC to their ballistic vest, as donning the vest typically signifies a shift to an enforcement capacity.
  - b. <u>Covert Employees</u>: Employees not permanently assigned to undercover roles but who occasionally assume a covert function are exempt from wearing and using their BWC during those specific instances. However, upon completing the covert assignment or when transitioning to an enforcement role, they must wear and use their BWC in accordance with this policy.

- c. Office of Professional Standards (OPS): OPS employees may choose not to wear a BWC during administrative or investigative activities related to their job function if they can reasonably articulate that doing so would adversely impact their investigation. However, in all other situations, OPS employees must adhere to this policy and wear their BWC in accordance with this policy.
- d. <u>Task Force Employees</u>: Employees assigned to a regional, state, or federal task force are required to wear and use their BWC in accordance with this policy unless prohibited by their respective task force policy. If a prohibition exists, the task force officer shall comply with this restriction to the extent explicitly restricted by the task force policy.
- e. <u>Class-A Uniformed Employees</u>: Employees wearing a Class-A Uniform are not required to wear a BWC as these uniforms are intended for non-operational and ceremonial activities.

### B. EXEMPTED AND/OR PROHIBITED RECORDINGS

- 1. Recordings that are exempted and/or prohibited from being recorded, fully or in part, are as follows:
  - a. <u>Surreptitious Recording</u>: <u>Employees are prohibited from</u> surreptitiously recording another employee of the NIH. If a BWC is recording, employees shall answer in the affirmative if other employees inquire if they are being recorded.
    - Although not required, employees should consider providing notification to other employees that a recording has been initiated [See 2.7 Audio/Video Recording Devices B.2].
  - b. <u>Division of Police Briefings</u>: <u>Employees are prohibited from recording DP meetings and briefings</u>, such as roll calls, planning sessions, performance discussions, tactical briefings, or similar internal meetings, unless authorized by a supervisor.
  - c. <u>Training</u>: Employees are prohibited from activating their BWC during training, except when explicitly authorized by a trainer or supervisor.
  - d. <u>Strip Searches</u>: Employees are prohibited from recording a strip search and shall maintain their device in Sleep Mode as the search is being completed. Once the search is complete, the member shall reactivate their device consistent with this policy.
  - e. <u>Bomb Threats</u>: Employees may, at their discretion, deactivate and power off their BWC when investigating bomb threats or suspicious packages under the same circumstances where utilization of the radio is prohibited due to concerns that radio transmissions could potentially cause a detonation.
  - f. <u>Interview Rooms</u>: Employees may, at their discretion, not wear/activate a BWC while conducting an interview in a room equipped with operating audio and video recording equipment, provided the equipment is functioning correctly.
  - g. <u>Command Functions</u>: Employees are prohibited from recording activities in and around a command post, command bus, emergency operations center, joint operations center, tactical operations center, negotiation operations center, or similar function unless

otherwise approved by an incident commander.

- h. <u>Attorneys</u>: Employees are prohibited from recording any conversations or discussions with attorneys regarding a pending/ongoing criminal or civil matter.
- i. <u>Undercover Officers and Confidential Informants</u>: Employees shall avoid, when practical, recording undercover officers and certified confidential informants who are performing activities on behalf of this DP or other law enforcement agencies.

# 2.8.09 SPECIAL LOCATIONS

1. Due to the sensitive nature that is inherent to certain locations, there is cause to modify recording practices to properly balance law enforcement objectives with community expectations. Employees shall abide by this policy while operating a BWC within a special location described below.

# A. NATIONAL INSTITUTES OF HEALTH DIVISION OF POLICE FACILITIES

- 1. BWC activation within secured portions of NIH Facilities police areas shall be limited to recording only events and activities explicitly required or permitted by this policy. Events and activities that may necessitate recording within NIH Facilities include interviews with suspects or witnesses, searches, arrests, or any other activity that may result in use of force, complaints, or recording requests. Recording of activities such as roll calls, tactical briefings, training, administrative investigations, employee wellness activities, meals, breaks, restrooms, and locker rooms is generally prohibited.
- 2. Employees are not required to wear their BWC within secured portions of NIH Facilities. If an employee elects to physically wear their device while within NIH Facilities, they shall maintain their device in Sleep Mode or Powered-Off Mode until after they exit the facility, or until there becomes a need to activate the camera pursuant to this policy [2.8.07A, Device Activation].
- 3. Employees are permitted to function-check their BWC momentarily within NIH Facilities or at their designated duty post.

# **B. CLINICAL CENTERS AND HEALTHCARE FACILITIES**

- 1. Recording in clinical centers or healthcare facilities is only permitted for reasons explicitly required by this policy [2.8.07A, Device Activation]. Discretionary recordings in these locations are prohibited.
- 2. Employees may deactivate their BWC while within clinical centers and healthcare facilities to balance individual privacy interests, provided that the patient has been accepted to the facility and medical/mental care has begun, and the patient is cooperative and/or adequately secured, with no foreseeable need for force beyond handcuffs or similar restraints.
- 3. Employees are responsible for continuously monitoring both the situation and any individuals in their custody and should reactivate their BWC as soon as possible if the need arises.

- 4. Employees are expected to exercise their best judgment when deciding whether to deactivate their BWC in a healthcare facility and should consult with a supervisor for guidance if necessary. However, they should also bear in mind that continuing to record may be the most prudent decision in some situations.
- 5. Employees shall resume recording once the treatment is over and the individual returns to the primary care and custody of the police department.

# C. CHILDREN'S INN, FACILITIES OCCUPIED BY JUVENILES, BSL LABARATORIES AND IRRADIATOR ROOMS

- 1. Recording in the Children's Inn or other facilities primarily occupied by juveniles is only permitted for reasons explicitly required by this policy [2.8.07A, Device Activation]. Discretionary recordings in these locations are prohibited.
- 2. Recording in the BSL laboratories, or irradiator rooms and other areas where strict security protocols are required is only permitted for reasons explicitly required by this policy [2.8.07A, Device Activation]. Discretionary recordings in these locations are prohibited.

# D. RESTROOMS, LOCKER ROOMS, AND DRESSING ROOMS

- 1. Recording in restrooms, locker rooms, and dressing rooms is only permitted for reasons explicitly required by this policy [2.8.07A, Device Activation]. Discretionary recordings in these locations are prohibited.
- 2. Employees entering these locations for non-law enforcement or personal reasons shall place their device in Sleep Mode and maintain the device in this mode until after they exit the location.

# E. ADULT AND JUVENILE DETENTION CENTERS

- 1. Employees are permitted to record within detention center facilities for law enforcement purposes unless such recording is explicitly prohibited by detention center rules.
- 2. Employees transporting an arrestee to the Montgomery and Ravalli County Adult Detention Center and Juvenile Detention Centers shall maintain their BWC device in recording mode throughout the transport, arrival, entering the sally port, and during the prisoner search process. However, if the search process involves a strip search, the required BWC operational mode outlined in 2.8.08B, Exempted and/or Prohibited Recordings, shall apply.
- 3. Once admitted to the facility, employees may deactivate their BWC device at their discretion. However, it is important to note that employees are still required to record suspect/arrestee interviews and interactions with the Magistrate when accompanied by the suspect/arrestee. [2.8.07A, Device Activation].
- 4. Employees shall keep their BWC activated while obtaining a breath sample following a DUI arrest, including during the observation period.

# F. COMMUNITY SHELTERS AND SUBSTANCE ABUSE TREATMENT CENTERS

1. Recording in community shelters, substance abuse treatment centers, and similarly

purposed locations is only permitted for reasons explicitly required by this policy [2.8.07A, Device Activation]. Discretionary recordings in these locations are prohibited.

## G. COURTHOUSE / COURTROOMS

- 1. BWC devices are prohibited in City, County, State, Federal courtrooms, and employees shall store them in the courthouse weapon lockers along with their firearms to comply with this prohibition.
- 2. Employees working in courthouses other than Federal must adhere to the policies established by the respective location.

# H. U.S. ATTORNEY, STATE'S ATTORNEY AND GENERAL COUNSEL

1. In order to safeguard sensitive activities within the U.S Attorney, State's Attorney and General Counsel's Offices, BWCs shall only be activated in these areas for events that are explicitly required by this policy [2.8.07A, Device Activation]. Discretionary recordings in all non-publicly accessible areas in these locations is prohibited.

## I. LOCALITIES WITH TWO-PARTY CONSENT LAWS

- 1. Some states, including Maryland and Montana, have two-party consent laws that prohibit recording or eavesdropping on confidential communications, such as private conversations or telephone calls, without the consent of all parties involved.
- 2. Employees performing activities outside the NIH campuses within the States of Maryland or Montana may use BWCs while performing lawful duties but shall proactively notify individuals being recorded unless it is unsafe to do so. Notification can be given by stating, "I am notifying you that this interaction is being audio and video recorded," or something functionally equivalent.
- 3. To safeguard sensitive activities within the Office of the State Attorney in Maryland and Montana, or in the NIH Office of General Counsel, BWCs shall only be activated for events that are explicitly required by this policy [2.8.07A, Device Activation]. Discretionary recordings in all non-publicly accessible areas in these locations is prohibited.

# 2.8.10 ACCESS TO BWC FILES

- 1. All BWC recordings, including images, videos, audio, and data, are the property of the NIH, DP. Employees shall not copy, publish, share, release, or disseminate any BWC recordings except to support a bona fide investigation to a law enforcement officer and or with the prior approval of the Chief of Police. Authorization by the Chief of Police or the designee acting in the Chief's absence is required to release BWC recordings to anyone other than a law enforcement officer.
- 2. Employees shall not edit, delete, or alter any BWC recordings stored on the cloud server or other storage media devices, except as authorized by the Chief of Police, or the designee acting in the Chief's absence.

### A. ACCESSING BWC FILES FOR LAW ENFORCEMENT PURPOSES

- 1. Employees are permitted to access their own BWC files solely for valid law enforcement purposes, including but not limited to report writing, court preparation, training, and investigative activities.
- 2. Employees may further access BWC files belonging to their colleagues, but only when it is essential for advancing an active criminal investigation. For any other reasons, such as report writing, court preparation, or training, access to a colleague's BWC file must be authorized by the file's owner and/or a supervisor.
- 3. While accessing a colleague's BWC files, employees must exercise the highest level of discretion and strictly limit access to the approved and intended purpose.
- 4. Employees must be aware that all access to BWC files is permanently recorded in the video audit log, which serves as an official record of employees who have accessed BWC files, including the date, time, and length of access. Unauthorized access or improper use of BWC files may result in disciplinary action.

# B. ACCESSING BWC FILES IN ADMINISTRATIVE INVESTIGATIONS [41.3.8c]

- 1. Employees are authorized to review their own BWC files before participating in internal investigations, such as administrative investigations, use of force investigations, administrative inquiries, unit-level inquiries, or other similarly purposed administrative investigations.
- 2. Employees may also be granted access to pertinent BWC files generated by a colleague, contingent upon obtaining prior authorization and being supervised by the case investigator. This access shall not be granted if it significantly and unjustifiably jeopardizes the integrity of an ongoing investigation, as determined by the case investigator. Employees who are denied access have the right to appeal this decision to the Chief of Police or a designated representative in the Chief's absence.
- 3. The investigation or interview will commence immediately following the BWC file review period unless a delay is authorized by the case investigator for a justifiable reason.

### C. ASSESSING BWC FILES IN EMPLOYEE-INVOLVED CRIMINAL INVESTIGATIONS

- 1. The DP is committed to ensuring that employees understand the legal distinctions between administrative reviews and criminal investigations and that the legal rights and due process protections of employees are respected in both contexts. Employees shall be reminded that the nature of a criminal investigation is to determine if any laws were violated and to identify the person/s responsible for the violation. [41.3.8c]
- 2. During any employee-involved criminal investigation, including those concerning critical incidents such as officer-involved shootings, employees are prohibited from accessing their own BWC files or that of their colleagues unless explicitly authorized by the case investigator and/or Chief of Police. This restriction serves to uphold the integrity of the investigation and safeguard the legal rights and due process protections of all parties involved.

### D. ACCESSING BWC FILES IN EMPLOYEE-INVOLVED CIVIL MATTERS

- 1. Employees are authorized to review their own BWC files prior to participating in a lawsuit or similarly purposed civil matter.
- 2. With prior approval from the Chief of Police or their designee, employees are authorized to review relevant BWC files created by other employees unless doing so would profoundly and unreasonably jeopardize court proceedings.

## E. USE OF BWC FILES FOR TRAINING PURPOSES

- 1. The DP recognizes that some employees may have concerns about utilizing their BWC files for training purposes, but also acknowledges the potential training value that it holds.
- 2. In instances where alternative resources are unavailable, trainers may submit a detailed memorandum requesting approval to use BWC files for training purposes to their respective Branch Commander. The Branch Commander will weigh the value of training against officer privacy interests to make a decision.
- 3. If the request is granted, the trainer must inform all involved employees of the intent to utilize the BWC files for training purposes. If any employees object, they have the right to appeal the decision to the Chief of Police. In such cases, the BWC footage may not be utilized until the Chief of Police reaches a final decision.
- 4. Field Training Officers/Supervisors may access and review BWC footage of their trainees without any limitations provided it is for the purpose of evaluating, coaching, counseling, training, or addressing performance deficiencies and has not previously been restricted by the Chief of Police.

# F. CONFIDENTIAL AND RESTRICTED BWC FILES

- 1. Safeguarding the confidentiality of BWC files is essential to ensure the integrity of investigations, uphold privacy rights, and prevent any negative repercussions resulting from unauthorized disclosure.
- 2. In certain cases, it may be necessary to classify specific BWC footage as "confidential" to safeguard the integrity of an internal or administrative investigation. Only the Chief of Police, Deputy Chief of Police, or the Commander of the Office of Professional Standards (OPS) has the authority to assign this classification. Once marked as confidential, the employee who designated the file as such assumes responsibility for controlling access and use of the file.
- 3. Designation of BWC footage as "restricted" may be appropriate for sensitive or delicate incidents, at the discretion of a supervisor. Supervisors may designate an incident as "restricted" and determine which employees, if any, may access the related BWC footage. Employees who encounter such incidents are encouraged to confer with their supervisor if they believe the situation warrants classification as restricted. Appeals of a restriction made by a supervisor can be made through the DP chain of command with final approval by the Chief of Police.

# 2.8.11 CRITICAL INCIDENTS

- 1. Upon becoming involved in a critical incident, as defined by DP policy, employees shall ensure their BWC is activated as soon as it becomes safe and practical to do so. Employees shall not deactivate their BWC until instructed to do so by a supervisor.
- 2. Supervisors responding to these incidents shall recognize these events are handled as criminal investigation until determined otherwise.
- 3. The supervisor is responsible to direct the involved employees to deactivate the BWC only after they have been escorted away from the immediate crime scene and there is no expectation that the employee will need to return to the crime scene. To ensure proper documentation, it is crucial for the supervisor to communicate this deactivation instruction with absolute clarity so it can be memorialized within the BWC file.
- 4. The involved employees shall keep the BWC on their person until retrieved by the case investigator or other staff members as designated by the Chief of Police, or his designee. As soon as practical, the collecting officer shall upload the BWC file and tag the video as confidential. The collecting officer may contact the BWC Program Coordinator for assistance.
- 5. Employees should be aware that critical incidents are investigated as both criminal and administrative investigations. To understand their access to BWC files, employees should refer to sections 2.8.10B and 2.8.10C of this policy. [41.3.8c]

## 2.8.12 SUPERVISOR RESPONSIBILITIES

- 1. Supervisors are responsible for ensuring that employees comply with this policy regarding the use, care, and maintenance of BWCs. While doing so, supervisors should understand that intentional deviation from the policy should not be viewed in the same light as unintentional mistakes. They should be aware of the potential consequences of noncompliance and take appropriate measures to address any violations.
- 2. Supervisors shall conduct periodic inspections of employee's BWC equipment and ensure it is properly affixed to their uniforms and fully operational. [41.3.8e]
- 3. Supervisors shall conduct periodic inspections of employee's BWC recordings to ensure that incidents are recorded in accordance with the requirements of this directive.
- 4. Supervisors shall plan for the battery life of BWC devices during lengthy incidents to ensure employee devices remain operational during the entirety of the incident.
- 5. Except in extraordinary circumstances (medical illness, injury, incapacitation, etc.) and where prior approval has been granted by the on-duty watch commander, supervisors shall ensure employees upload BWC files at the end of their shifts and appropriately categorize their files.
- 6. Supervisors are prohibited from conducting routine reviews of BWC files and may only review the files of other employees to ensure compliance with recording requirements or

when there is sufficient cause, as outlined in this policy.

- 7. Supervisors are required to review relevant BWC files when employees under their supervision are involved in or alleged to be involved in actions, activities, or events that involve law or policy violations, the application of force, injuries, or death of an individual, employee injury, property damage, or vehicle pursuits. With commander approval, supervisors may further review BWC files when they have articulable justification that such review is necessary to address employee conduct, performance, training needs, afteraction review, or award commendation.
- 8. If a community member expresses a complaint or concern regarding an employee, the employee's supervisor should consider providing the complainant with an opportunity to view the relevant BWC file. This approach can potentially clarify the situation and prevent unnecessary investigations. However, if the supervisor believes that this approach may not be suitable or may not serve the best interests of the investigation, the supervisor should refer the complainant to other options such as the Discovery and/or Freedom of Information Act (FOIA) to obtain the BWC files.
- 9. Upon supervisor review of a BWC file for any of the reasons mentioned in this section, that supervisor shall document the purpose of the review and retain this documentation within the employee's squad folder for a period of one year. All reviews are also memorialized in the video audit trail.
- 10. Supervisors shall be alert to situations where BWC files should be designated as confidential or restricted and ensure that appropriate notifications are made to properly handle the files. They should also make themselves available to consider requests from officers or detectives to make videos restricted and respond in a timely and appropriate manner.

# 2.8.13 BODY-WORN CAMERA SECTION RESPONSIBILITIES

- 1. The BWC Coordinator is responsible for managing and administering the BWC program, including all associated equipment and software.
- 2. Management and administrative duties include, but are not limited to, issuing BWC equipment and training end-users, coordinating maintenance and warranty service with the vendor, function checking the system and files, providing technical assistance, coordinating repair and replacement of systems, conducting annual inspections, audits, assisting in responding to public records requests and redacting BWC files as necessary or as required by law, providing statistical and analytical support, assisting with on-scene uploads, file restriction, and forensic review of BWC files, addressing accidental recordings, and coordinating with outside departments such as the States Attorney's Office, and Information Technology.

# 2.8.14 COURT PROCEDURES

# A. U.S. ATTORNEY, AND GENERAL COUNSEL'S OFFICE

1. The Office of the U.S. Attorney, and the NIH General Counsel may have restricted access to BWC files and only to the extent that their respective offices are prosecuting, defending,

or are a stakeholder in a specific incident.

## **B. COURT PREPARATION**

- 1. When the Office of the U.S. Attorney, State's Attorney or NIH General Counsel has entered their appearance, they are responsible for coordinating the preparation of BWC files for trial.
- 2. Officers are reminded that any recording of a crime may be considered exculpatory evidence and subject to discovery in court proceedings. Therefore, documentation should be included in reports indicating the existence of the recording and notice should be given to any prosecutor handling the case. Notwithstanding these requirements, in cases where the U.S. Attorney, or NIH General Counsel has not noted their appearance, NIH employees may use their discretion to determine whether to present BWC footage as evidence or rely solely on their witness testimony. Efficiency in court proceedings should be taken into consideration when making this decision.
- 3. If an employee intends to present BWC files in court, they must notify the AUSA or prosecutor in advance and coordinate with court administrative personnel to share the BWC video through court room displays. To ensure a clear and efficient presentation, employees must review and prepare their files in advance, ensuring they are organized and ready for relevant and efficient presentation.
- 4. Defendants seeking access to BWC files should be instructed to request access through the AUSA or prosecutor through discovery. However, employees may, at their discretion, allow a defendant of non-jailable offenses to view relevant BWC files on a DP desktop or laptop computer to avoid unnecessary court delays.

# 2.8.15 PROVISIONS OF BWC FILES

### A. DISCOVERY

UNITED STATES

1. The U.S. Attorney's Office, or NIH General Counsel with the assistance of the DP have primarily responsible for fulfilling discovery requests. The DP and BWC Coordinator shall assist U.S. Attorney's Office, or NIH General Counsel in fulfilling this obligation.

## **B. SUBPOENA AND COURT ORDERS**

- 1. The BWC Coordinator will review BWC data when requested by subpoena or court order, and the BWC Coordinator will be responsible for coordinating with the AUSA and/or prosecutor to provide BWC video in accordance with applicable laws and procedures.
- 2. If sensitive information is included in BWC files ordered for release by subpoena or court order, the BWC Coordinator shall notify the Chief of Police, General Counsel, and/or U.S. Attorney to take precautions to protect those involved.
- 3. If the BWC Coordinator receives a subpoena or court order related to a pending criminal case from anyone other than the U.S. Attorney, the BWC Coordinator shall notify the prosecutor assigned to the case before complying to determine if any legal action should be taken prior to compliance.

### C. MUTUAL AID AND SHARING OF BWC FILES

1. Outside law enforcement agencies may request BWC footage related to criminal investigations. The BWC Coordinator may authorize approval for officers to share BWC files if the request supports a bona fide criminal investigation. If the BWC Coordinator has concerns about releasing the footage, they shall communicate their concerns through the chain of command to the Chief of Police prior to approving the release. While footage may be released unredacted, the privacy of parties involved, and DP interests must be protected. Any mutual aid requests related to administrative matters should be brought to the attention of the Body-Worn Camera Coordinator for review and request for release approval by the Chief of Police.

### D. MEDIA RELEASE

1. BWC files cannot be released to the media without the prior approval of the Office of Research Services Director and/or the Chief of Police, or their designee acting in their respective absence. When BWC data is approved for media release, privacy of all parties, criminal investigations, and NIH interests shall be protected. Audio may be redacted to mask personal, financial, medical, security and sensitive information. Redaction software should be used to blur faces, skin, addresses, license plates, or any sensitive materials that could compromise an investigation or place individuals in danger. When footage is released for identification purposes, only footage that can aid in the effort shall be provided with great care.

# E. FREEDOM OF INFORMATION ACT (FOIA)

- 1. Recordings from BWCs may be subject to release pursuant to the Freedom of Information Act, 5 U.S.C. 552. Any FOIA requests for the release of BWC recordings submitted to the DP will be forwarded to the BWC Program Coordinator (BWCPC), who will coordinate with the NIH FOIA Office to release recordings in an expeditious manner, considering any applicable FOIA exemptions required by 5 U.S.C 552 As Amended by The Freedom of Information Reform Act of 1986.
- 2. Not all records are required to be released under the FOIA. Congress established nine exemptions from disclosure for certain categories of information to protect against certain harms, such as an invasion of personal privacy, or harm to law enforcement investigations. The FOIA authorizes agencies to withhold information when they reasonably foresee that disclosure would harm an interest protected by one of these nine exemptions.

# a. Exemptions # 6 and 7 are:

- Exemption 6: Information that, if disclosed, would invade another individual's personal privacy.
- Exemption 7: Information compiled for law enforcement purposes that:
- o 7(A). Could reasonably be expected to interfere with enforcement proceedings.
- 7(B). Would deprive a person of a right to a fair trial or an impartial adjudication.
- o 7(C). Could reasonably be expected to constitute an unwarranted invasion of personal privacy.

- 7(D). Could reasonably be expected to disclose the identity of a confidential source.
- o 7(E). Would disclose techniques and procedures for law enforcement investigations or prosecutions or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.
- 7(F). Could reasonably be expected to endanger the life or physical safety of any individual.
- 3. The Privacy Act provides safeguards for individuals against an invasion of personal privacy through the misuse of records by federal agencies. The Privacy Act balances the individual's personal privacy interest against the Government's need to maintain information about individuals.
- 4. All BWC files shall be securely stored consistent with the Federal Records Act (FRA) and the retention schedules for law enforcement records recordings that have administrative or evidentiary value will be retained consistent with the General Records Schedule 5.6. Security Management Records and General Records Schedule 09, Operations and Facilities Management 09-430
- 5. BWC footage may be requested through FOIA, and the NIH FOIA Office will assist in processing FOIA requests. When an investigation or a court proceeding is ongoing, the request may be denied if it compromises the criminal justice process or falls under another FOIA exemption. When the Chief of Police or their designee approves the release of BWC footage, it may be appropriately redacted, using software to blur faces, skin, addresses, license plates, or other sensitive materials. Great care shall be taken when releasing BWC data as a result of a FOIA request to avoid compromising criminal investigations, violating citizens' privacy, or affecting NIH interests.

### F. EXPUNGEMENT

1. The BWC coordinator is responsible for reviewing, processing, and deleting any items subject to an Expungement Order. The review will confirm the number of suspects involved in the case. If the person named in the order is the sole suspect, all evidentiary items related to that case will be deleted in accordance with the order. If multiple suspects are involved, only the expunged person's identifying information will be redacted from related items, and the redacted version depicting the non-expunged suspects will be retained. Any deleted items will be noted as per court-ordered expungement.

# G. PUBLIC RELEASE OF BWC FILES INVOLVING CRITICAL INCIDENTS

- 1. Releasing BWC files of a critical incident can increase transparency and accountability in police actions, safeguard public trust in the DP, and provide a clearer understanding of the events leading up to and during the incident.
- 2. BWC recordings are redacted as necessary to preserve privacy rights, and released consistent with applicable legal processes or laws that pertain to public records requests and exempt certain types of records from public disclosure.
- 3. Determinations about whether or when to release critical incident BWC video shall be at the discretion of the Chief of Police after consultation with the AUSA. Notwithstanding

this requirement, the DP shall make every effort to release BWC files of critical incidents to the public within 20 business days, with earlier release possible at the discretion of the Chief of Police, or the designee acting in the Chief's absence.

- 4. Additional information providing context based on the evidence available at the time of release shall accompany the video's release.
- 5. There may be circumstances that require delaying video release to protect the safety of involved individuals, the integrity of an active investigation, confidential sources or investigative techniques, or the constitutional rights of the accused.
- 6. Any decision to withhold video beyond 20 days shall be reassessed every 10 days and based on specific factual grounds. If sufficient cause is established, video files may never be released.
- 7. Notifications shall be made to inform involved employees, subjects, and their representatives, as well as the Office of the U.S. Attorney, States Attorney or NIH General Counsel prior to releasing video imagery, absent exigent circumstances.
- 8. The release of any specific BWC file does not waive the DP's right to withhold other BWC files or investigative materials in the same or other cases, as permitted by law.

# 2.8.16 CLASSIFICATION, RETENTION, AND DOCUMENTATION [CALEA 41.3.8 d]

- 1. Officers will document in the narrative of their reports the fact that an incident was recorded on BWC or if video is not available, officers will document in the narrative of their report this fact and the reason video is unavailable.
- 2. BWC recordings are public records, and as such are subject to disclosure through the Freedom of Information Act (FOIA). Requests for recordings through FOIA will be directed to the NIH FOIA office for response. BWC video may be released at the discretion of the Chief of Police or upon receipt of the FOIA request.
- 3. Officers will correctly label all BWC videos with all available ID, Title, and Category Information. The correct labeling for each is:
  - a. **ID:** The associated CAD generated incident report number.
  - b. **Title:** In order of preference: victim name, primary suspect name, other relevant party name, or (only when no names are available) the incident address.
  - c. Category: Select all from the list that apply. Category will not be left as "None." Category selection will be based on the incident regardless of the individual officer's level of involvement.
- 4. Data from BWCs will be stored through use of approved, vendor-provided storage solutions with AXON's Evidence.com or as otherwise directed by the Chief of Police.
- 5. BWC recordings that have administrative or evidentiary value will be retained in accordance with the National Archives Records Retention Schedule, General Records Schedules (GRS), 5.6 Security Management Records and General Records Schedules (GRS), (9). Employees will log BWC videos into one of four categories for retention purposes, as follows:

- a. <u>Category 1: Accidental/False Activations</u>: This category is specifically designed for instances of unintentional or false BWC activations. Records are retained according to appropriate GRS schedules, a minimum retention period of 180 days, or six months.
- b. <u>Category 2: Formal Contacts with No Criminal Activity</u>: This category pertains to BWC activations during law enforcement interactions, including but not limited to traffic stops, subject checks, and service calls that do not involve any actual or suspected criminal activity. Records are retained according to appropriate GRS schedules, with a minimum retention period of three years or 1,095 days.
- c. <u>Category 3: Formal Contacts Involving Actual or Suspected Misdemeanor Crimes:</u> This category includes any BWC activation related to an official law enforcement contact involving an actual or potential misdemeanor offense. Records are retained according to appropriate GRS schedules, a minimum retention period of five years or 1,825 days,
- d. <u>Category 4: Formal Contacts Involving Actual or Suspected Felony Crimes</u>: This category includes any BWC activation during an official law enforcement contact involving an actual or potential felony offense. Records are retained according to appropriate GRS schedules, with a minimum retention period of 9,125 days or twenty-five years.

Category 4 recordings that meet requirements for permanent retention as determined by the Chief of Police will be copied to a DVD or other external storage device and placed into evidence for long term storage by the BWC Coordinator.

Retention periods for any BWC evidence in any of these categories may be extended upon the order of a court with jurisdictional authority over the related court case.

- 6. If an employee becomes aware that the significance of an incident has changed since the original categorization of the BWC file, they must make the necessary changes to ensure the file is retained appropriately and in accordance with the law. If a BWC file is re-classified to a different retention category (e.g., non-evidentiary to evidentiary), the recording will be subject to the retention category with the longest retention period.
- 7. NIH shall preserve all recordings related to any criminal proceeding, claim filed, pending litigation, or administrative investigation until the matter is resolved or as required by applicable laws, whichever is greater.
- 8. Categories and retention periods for BWC files may change if the Federal Government updates the GRS retention schedules. All BWC recordings will be assigned a retention category, and after the retention period is over, the recordings will be expunged from the DP's system in accordance with the record destruction procedures established by the Federal Government.
- 9. As stated in 2.8.07D, Accidental Recordings, if a BWC is accidentally activated and the resulting recording serves no law enforcement or administrative purpose, employees may submit a deletion request to their immediate supervisor for approval. The request should include sufficient information to locate the recording, along with a brief narrative explaining the reason for deletion. Upon receiving a deletion request, the BWC Section Supervisor will evaluate the associated BWC file to ascertain if it holds any official law

enforcement or administrative value. If the recording is deemed purposeless, the BWC Section will proceed with its deletion and document the action in an audit log. In exceptional cases where an employee is uncomfortable having their BWC file reviewed by a BWC Coordinator due to the presence of personally sensitive content, the employee may request an alternative method to protect the privacy of the BWC file. Within their request, the employee should state their privacy concerns and provide a general description of the contents of the BWC file (e.g., "device activated while inside a locker room"). The employee may make a written request that the file be designated as restricted and made inaccessible without the BWC Coordinator's approval. This request does not guarantee that the recording will remain unexamined if it is later alleged to be relevant to a law enforcement or administrative purpose.

# 2.8.17 PROCEDURES FOR FREEDOM OF INFORMATION ACT REQUEST

FOIA requesters interested in obtaining information on an NIH, Division of Police Body Worn Camera, or Police Report under the Freedom of Information Act shall:

Submit the FOIA request by email to erin.holden@nih.gov or by letter to:

Attention Privacy Coordinator Erin Holden, Management Analyst, and Review Branch, 31 Center Drive, Building 31, Room, 4B30, MSC 2140, Bethesda,

Reasonably describe the information being sought, if you want information about yourself, you will be required to provide proof of your identity, to protect your privacy, and ensure YOUR privacy information is not disclosed to someone else.

For questions regarding FOIA contact Erin Holden at (301) -827-8198