DEPARTMENT OF CORRECTIONS

Policy Number:	**301.037**
Title:	**Body-Worn Cameras (BWCs)**
Effective Date:	**12/02/24**

PURPOSE:
To provide procedures for the use of body-worn cameras (BWCs) by correctional facility staff and intensive supervised release (ISR) agents in order to promote safety and transparency, and to document events for the protection and safety of staff and those served by the department.

APPLICABILITY:
Pilot project implementation for listed staff: uniformed facility security and transportation personnel and ISR agents. This policy does not apply to the Office of Special Investigations Fugitive Apprehension Unit, which is subject to DOC Policy 107.019, "Office of Special Investigations – Fugitive Apprehension Unit – Body Worn Cameras."

DEFINITIONS*:*
Body-worn camera (BWC) administrator – person who is authorized and trained in the operational use and repair of BWCs, including procedures for duplication, storage, and retrieval processes, and who possesses a working knowledge of video forensics and evidentiary procedures.

Body-worn camera (BWC) audio/video – audio-video signals recorded on any storage device obtained through a department-installed BWC system.

Body-worn camera (BWC) system – any system that captures audio and video signals, capable of being worn individually by a user.

Buffer – a configured component of the BWC that records a preset timeframe prior to an event activation. The buffer records only when the BWC is powered on. Audio recording begins when the user tags live data for event activation. The buffer sequence becomes a part of the tagged event.

Critical incident – any incident that has caused or is likely to have caused great bodily harm or death to any person.

Event activation – any process that causes the BWC to start tagging currently recording audio or video data for preservation at the start of the event.

Event deactivation – any process that causes the BWC to stop tagging currently recording audio or video data at the end of the event and requires the user to select a predetermined tagging category.

Great bodily harm – see Policy 301.081, "Response to Resistance, Restraint Systems, and Escape."

Intensive supervised release (ISR) – a supervision level closely monitoring and managing high-risk individuals in the community after they are released from prison under supervision.

Mandatory recording – when the BWC must be powered on under this policy.

Prohibited recording – when a user is not allowed to have the BWC powered on under this policy.

Tagging – an automatic system within the body worn camera software which marks a video frame when a user starts and ends a recording.

Unintended recording – when a user captures audio and video data because the user is unaware the BWC was powered on.

User – A DOC staff member who is required by this policy to wear a BWC.

PROCEDURES:

A. **Operational Objective**

The DOC has adopted the use of body-worn cameras (BWCs) to accomplish the following objectives:

1. To document interactions and events between staff and incarcerated people, or those subject to intensive supervised release (ISR.)

2. To enhance staff's ability to document and review client interactions for internal reporting requirements, complaint/violation/discipline proceedings, or for courtroom preparation/presentation.

3. To preserve visual and audio information for use in current and future processes, including investigations, violation hearings, disciplinary proceedings, and judicial proceedings.

4. To enhance the public trust by preserving factual representations of interactions between staff and incarcerated persons/high-risk individuals in the community in the form of video and audio recordings. (See section P.2., below.)

5. To identify staff training needs and to conduct after-action or post-incident reviews.

6. To protect both department of corrections (DOC) staff and clients from incomplete, unjustified, or falsified complaints.

B. **Responsibilities Related to the Use of BWCs – All Users**

1. Users must wear their BWCs with agency provided attachment devices, and in accordance with training and generally accepted standards that afford the maximum possible view.

2. The user is responsible for the inspection and general maintenance of the BWC equipment issued to them.

3. At the start of each shift, the assigned user must perform an inspection to ensure the BWC is operating in accordance with the manufacturer's recommendations and DOC specifications. If a user is unable to perform the inspection at the start of their shift due to an emergent incident response need, the user must perform the inspection as soon as practicable and make a notation in their incident report indicating the inspection was performed after the incident response was completed.

4. Users may be requested or required to work in areas without access to BWC docking station capability. If the user does not have the ability to upload the information from the BWC, the user must complete an upload during the next shift where a docking station or working department laptop is available.

5. Users must inform those who ask that recording equipment is in use.

6. Users may not use the muting function on the BWC.

7. Under no circumstances may a user personally sell, transfer, share, access, or distribute audio or video recordings without express and written permission of the commissioner of corrections or their designee.

8. Subpoenas or other requests for recordings for purposes of criminal investigation, prosecutor review, or discovery must be referred to and processed by the BWC administrator.

9. Data requests for audio/video recordings must be directed to the BWC administrator and, if media-related, to the public information officer for a response consistent with the Minnesota Government Data Practices Act (MGDPA).

C. **Issuance**

1. All staff assigned BWCs must successfully complete training in the use of the technology and this policy. Training is documented in the agency-approved electronic training management system.

2. One BWC must be checked out by a user prior to shift start.

3. Users may not switch or trade BWCs between each other. The person to whom the BWC has been checked out must use the same BWC throughout their shift and check it back in and dock it before leaving the facility.

4. Field Services staff are assigned a permanent BWC system.

D. **Additional Responsibilities Specific to Facility Users**

1. Facility users must dock the BWC units after the completion of their shift.

2. Facility users must promptly report any malfunctions or damage of BWC equipment to their supervisor and complete a BWC administrator notification form documenting the non-functioning BWC, prior to placing the unit into service. If the BWC is damaged during duty, the circumstances must be documented in an incident report, with a copy provided to the BWC administrator. The supervisor, watch commander, or BWC administrator must provide direction to the user regarding replacement if the damage affects the audio and video recording capability of the device.

3. Transportation personnel users are responsible to dock (upload) their BWC as is practicable, following any transport. Transport personnel involved in an incident of significance (for example, escape, attempted escape, or other notable incident) must notify their immediate supervisor and must upload the BWC only as directed by the investigating law enforcement authority, if any, or as soon as practicable at the conclusion of the user's shift.

E. **Additional Responsibilities Specific to Field Services Users**

1. Field services users must upload the contents from the BWC on their department-issued laptop through cloud computing following a client field visit, or after the completion of their shift.

2. Each field services user is responsible to dock (upload) their BWC as soon as practicable following any enforcement activity, such as observed conduct depicting a violation of the

conditions of supervised release, arrest, or other event of significance that does not meet the criteria of a critical incident.

F. **BWC Use – Facilities**

1. Facility users must wear, power on, and use their assigned BWC any time they may have interactions with an incarcerated person or during assignments which place the staff in an area currently populated by incarcerated people. BWC use may only cease when recording is prohibited or when sleep mode is authorized. The BWC must be powered on during the following activities:
   a) While working in a housing unit control bubble;
   b) While transporting an incarcerated person/resident; and
   c) While performing an unclothed body search pursuant to an A-Team response and placement in restrictive housing.

2. Facility Incident Event Activation and Video Tagging/Retention/Documentation:
   Any time a user is required to prepare a report regarding an incident, the user must document the actual or approximate incident start and end times in their report. The times when the activation of event tagging is necessary include such examples as:
   a) When interacting with aggressive or agitated individuals;
   b) Escorts determined by the managing officer, including any escort from a use of force event;
   c) Any time the wearer, at their own discretion, feels threatened, harassed, or unsafe.
   d) Vehicle transports when incarcerated persons/residents become aggressive or disruptive, experience medical emergencies, or require unscheduled vehicle stops; and
   e) When directed by a supervisor.

3. Facility users must activate event tagging for the entirety of an incident and should only deactivate event tagging at the direction of a supervisor.

4. All event taggings, regardless of type, will result in capturing the buffering time. The buffering time for the BWC must be 90 seconds with video and sound.

5. Automatic activation of event tagging may occur in the following instances if a Bluetooth signaling device is installed and triggered, including:
   a) When oleoresin capsicum (OC) spray is removed from a holder which has a Bluetooth signaling device; and
   b) When Bluetooth signaling is triggered upon deployment of other equipment such as a Taser device.

6. The user may deactivate the BWC event tagging:
   a) Following a critical incident, and only when the investigating entity, appointing authority, or their designee has directed event deactivation; and
   b) When event deactivation is directed by the commissioner of corrections or their designee.

7. A user's decision to deactivate event tagging in a situation that would otherwise be tagged under this policy must be documented verbally on the camera before the deactivation of event tagging on the BWC.

G. **BWC Use - Field Services**

1. Field Services users must wear, power on, and use their assigned BWC during client field or office visits.

2. Field Services Event Activation and Video Tagging/Retention Documentation:
   Any time a user is required to prepare a report regarding an incident, the user must document the actual or approximate incident start and end times in their report. Event activation includes such examples as:
   a) Witnessing conduct that constitutes a violation of the conditions of supervision;
   b) Incidents where the user feels threatened, harassed, or unsafe, unless otherwise prohibited by this policy;
   c) Interacting with aggressive or agitated individuals, including non-clients, while engaged in field supervision activities;
   d) During periods of detention, directed by the agent, pending arrest by law enforcement personnel;
   e) During agent observed law enforcement actions such as arrest;
   f) Vehicle transports of clients; and
   g) When directed by a supervisor.

3. Field Services users must consider the totality of the circumstances before deactivating event tagging.

4. All event tagging, regardless of type, results in capturing the buffering time. The buffering time for the BWC must be 90 seconds with video and sound.

5. Automatic activation of event tagging may occur if a Bluetooth signaling device is installed and triggered when OC is removed from a holder which has a Bluetooth signaling device.

H. **Discretionary Event Activation**

1. This policy does not describe every possible situation when a user may activate event tagging. Except when event recording is prohibited under this policy, a user may use the BWC for event tagging whenever they believe it is applicable based on their training, experience, and judgment.

2. If a user is involved in a situation and they are unsure if event tagging is mandatory, discretionary, or prohibited, they should activate event tagging on the BWC.

I. **Exceptions to Mandatory Event Activation**

1. In a sudden or dangerous event in which a user would be unable to use the BWC to activate event tagging, the user must activate event tagging as soon as practicable.

2. Event tagging may not be possible when there is a BWC equipment failure that is properly reported pursuant to Section C, and for which there is no immediate remedy.

J. **Sleep Mode Authorization**

1. The BWC must be placed in sleep mode in the following situations while a user is performing their job duties:
   a) During a probation or performance review;
   b) During a meeting or training;
   c) During official duties by a union representative;
   d) While interviewing a current or potential confidential informant;
   e) While present in a court of law;

f) During a routine unclothed body search (searches immediately following a use of force event are still part of that event and BWCs should remain on event activation until the end of the event); and
g) Where legally required to do so, or when directed to by a supervisor.

K. **Prohibited BWC Use**

1. Users must not have their BWC powered on in the following situations:
   a) During a non-work-related activity;
   b) Within areas of a facility/office restricted to personnel-only access, including meeting rooms, staff offices, locker rooms, break rooms, and report rooms;
   c) During a work break;
   d) At any location where a reasonable expectation of privacy exists, such as a bathroom or locker room, unless necessary as part of an exigent or emergency incident response;
   e) In patient care areas of a hospital, sexual assault treatment center, or other healthcare facility unless necessary for an incident response (if an event is activated due to an incident response, it must be deactivated once the incarcerated person is compliant and non-resistant);
   f) In treatment groups;
   f) During administrative meetings or discussions;
   g) During conversations involving privileged communication (for example, attorney/client visits, interactions with clergy);
   h) During any official inquiry regarding employment (for example, administrative investigations or pre-discipline hearings) or when providing representation or serving as a witness on behalf of an employee during an official inquiry regarding employment;
   i) During unclothed body searches of a compliant incarcerated person, unless articulable factors such as aggression, attempts to conceal, etc., are present; and
   j) Due to Prison Rape Elimination Act (PREA) related considerations providing privacy to clients while using the restroom (including during the collection of an observed urinalysis), showering, and while receiving medical treatment, during the examination of genitalia, breasts, etc.

2. This policy recognizes that users may create unintended or prohibited recordings. If an unintended or prohibited recording has occurred, the user must prepare a report describing the unintended or prohibited recording including the time of the incident, which shall be forwarded to the BWC administrator for deletion. Once completed, the BWC administrator shall notify the user that the preserved video has been deleted from the system.

L. **Power-Off Authorization**

1. Except at the end of a shift/workday or the end of field work, an employee must not power off a BWC except as listed in section K, above or authorized by a supervisor.

2. Exception –an employee may use the sleep mode when using the restroom/locker room to safeguard their own privacy, and they may also power off the BWC system if they prefer. However, they must power it back on immediately after leaving the restroom/locker room.

M. **BWC System Recorded Data**

1. Evidentiary Value
   Whenever an audio or video recording documents a critical incident that may be subject to investigation by law enforcement authorities, the recording constitutes evidence and should be handled accordingly. As such, care must be given to documenting and maintaining a

chain of custody and ensuring the integrity of any video or audio recordings. Recordings can include tagged event recordings, buffer recordings, or routine recordings not tagged for event recording. (See also Policy 301.035, "Evidence Management.")

2. Facility Users – Critical Incidents
   a) When a critical incident occurs and a user is unable to bring the BWC to a docking station, a supervisor or designee must respond to the scene and secure all BWCs once the incident has concluded, and staff are away from the location of the critical incident.

   b) The supervisor or designee must then dock the BWCs in a location directed by the watch commander under the supervision of supervisory personnel who must prepare a report documenting the download of the relevant BWC data. The watch commander must immediately inform the BWC administrator of the download. The administrator must place the recording(s) in a secure file that only authorized personnel can access.

   c) Users are not allowed to view the critical incident footage unless and until approved to do so by the commissioner of corrections.

   d) The DOC's chief law enforcement officer, in consultation with the commissioner, may assign a critical incident to an outside agency for investigation.

   e) If an investigation is to occur, a user may request to review their BWC video with the assigned investigator, but only after an initial interview. Once the user has reviewed their BWC video, the interview process may continue.

3. Field Services Users – Critical Incidents
   a) Should an agent witness or be involved in a critical incident, a supervisor or designee must respond to the scene and secure any BWC from the user once the incident has concluded, unless the BWC is required by an investigating law enforcement entity.

   b) The supervisor or designee must then dock the BWC in a location directed by the supervisory personnel who must prepare a report documenting the download of the relevant BWC data. The supervisor must immediately inform the BWC administrator of the download. The supervisor must place the recording(s) in a secure file that only authorized personnel can access.

4. Protection and Audit of Data
   a) Review of Data:
   Audio and video recordings generated in connection with a user's duties are the exclusive property of the Minnesota DOC and are not available for external use, except as provided by this policy and in accordance with state law.

   b) Viewing of BWC Recordings:
      (1) The video storage platform has integrated auditing. View and access attempts are tracked at the individual level.

      (2) Access to BWC recordings must be for legitimate purposes only. Any time video is accessed, the person accessing the video must make a notation

identifying the reason for the video being accessed (for example, routine audit, case investigation, supervisory review, etc.).

(3) The BWC administrator, DOC legal counsel, authorized DOC staff (field services director, facility captain), and authorized DOC data practices personnel may access BWC data in order to complete their duties. Internal or supervisory audits and reviews are mandatory to ensure compliance with policy and law.

(4) Other DOC staff may review a BWC recording with specific approval from the commissioner of corrections, for training or incident review purposes.

(5) An outside law enforcement agency with a bona fide or investigatory need to know may review a BWC recording upon request and approval from the DOC's chief law enforcement officer or designee.

(6) Users are not allowed access to their own BWC data, except as described within this policy for legitimate purposes.

(7) Data must be made available to prosecutors, courts, defense attorneys, the hearing & release Unit, and other criminal justice entities as provided by law.

(8) Data may be available in compliance with Minnesota data practices laws, including the public benefit section of Minn. Stat. § 13.85.

(9) The DOC presumes a public benefit in allowing family members (representatives of the decedent) to view BWC recordings of any deadly force encounter and must facilitate such viewing within five days of an event, upon request of a qualified representative.

(10) PREA standards dictate specific requirements with regard to viewing data, specifically the general requirement for same-sex viewing. Opposite gender staff who are not involved in a specific investigation are prohibited from viewing any recorded video of naked clients, bathing clients, clients using the restroom, etc. However, managers and supervisors of opposite genders are allowed to review videos for the sake of a use-of-force review.

N. **BWC Data Retention**

1. All audio/video recordings must be maintained in accordance with the MGDPA and the records retention schedule.

2. All tagged audio/video recordings must be maintained in accordance with the agency's records retention schedule.

3. Upon written request of the subject of BWC data, the DOC will retain relevant BWC video beyond the normal retention period, up to 180 additional days. At that time, untagged video/audio data will be destroyed, unless a new request is made.

O. **Misuse of Equipment or Recordings**

Users who do not use the equipment as outlined in this policy, or who misuse recorded data, are subject to disciplinary action up to and including termination. If the misuse rises to the level of

criminal conduct, the office of special investigations (OSI) will investigate or refer the matter to an appropriate law enforcement agency for investigation.

P. **The BWC Administrator:**

1. Coordinates and responds to data requests regarding BWC audio/video recordings;

2. Reviews all recordings prior to public release to ensure compliance with Minnesota data practices laws;

3. Arranges for an independent audit of BWC data once every two years and ensures the audit results are provided to the director of OSI. Also arranges and conducts internal audits of BWC data twice annually to ensure consistent data management practices across the agency in accordance with Minnesota data practice laws, data retention schedules, and this BWC policy. Additionally, the administrator must provide a report of audit findings to the commissioner of corrections, the DOC's chief legal counsel, and the inspector general; and

4. Maintains the following public BWC data:
   a) The total number of devices owned by the agency;
   b) The total number of devices that are actually deployed and used;
   c) The policies and procedures for use of BWCs; and
   d) The total amount of recorded audio/video data collected by BCAs and maintained by the agency, the agency's retention schedule, and the agency's procedures for destruction of the data.

INTERNAL CONTROLS:

A. User training in the use of BWCs is documented in the agency-approved electronic training management system.

B. Any malfunctions or damage of BWC equipment is documented within an incident report, which is retained at the facility.

C. All facility audio/video recordings are retained in accordance with the Minnesota Government Data Practices Act and the agency's records retention schedule. Upon written request of the subject of BWC data, the DOC retains relevant BWC video beyond the normal retention period, up to 180 additional days, at which time a new request would need to be made.

D. The BWC administrator retains all documentation related to BWCs.

REFERENCES: Minn. Stat. Chapter 13 (Minnesota Government Data Practices Act)
Policy 107.019, "Office of Special Investigations – Fugitive Apprehension Unit – Body Worn Cameras"
Policy 301.035, "Evidence Management"
Policy 301.081, "Response to Resistance, Restraint Systems, and Escape"

REPLACES: All facility policies, memos, or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

ATTACHMENTS: None

APPROVAL:
Commissioner of Corrections