POLICY DIRECTIVE

Policy:	**DOC 3.1.27 CAMERA SURVEILLANCE SYSTEM**
Effective Date:	04/28/2017 Page 1 of 3
Revision Date(s):	04/24/2026
Signature/Title:	/s/ Eric Strauss, Director

I. POLICY

The Department will ensure camera surveillance is conducted in a manner consistent with legal requirements and establish guidelines for the appropriate use of surveillance within or on the grounds of a Department facility, office, or building.

II. APPLICABILITY

All Department divisions, facilities, and programs.

III. DEFINITIONS (see Glossary)

IV. REQUIREMENTS

A. General Guidelines

1. Surveillance cameras are used in Department facilities, offices, and other buildings to ensure safe, secure, and humane operations.
   a. They will only be used by authorized individuals and only for approved Department business purposes.
2. Division chiefs and facility administrators are responsible for managing camera surveillance systems in accordance with this policy.
3. In accordance with *DOC 1.1.17 Prison Rape Elimination Act (PREA)*, when surveillance cameras or the associated monitoring software are installed or updated in a Department facility, the facility PREA Specialist and the Department PREA Coordinator will be consulted to consider how the camera and software technology may enhance the Department's ability to protect inmates from sexual abuse.
   a. This consideration will be documented in writing and retained by the Department's PREA Coordinator.
4. Employees who misuse camera surveillance equipment or video images will be subject to disciplinary action. Misuse includes disseminating images without proper authorization, viewing video footage to satisfy curiosity, or other violations of this policy.

B. Purchasing, Installation, and Maintenance

1. To maintain necessary camera equipment and software technology, all surveillance cameras, servers, and/or associated software and hardware purchases for the Department will require prior approval from the Information Technology CIO or designee.
2. The location, viewing area and/or camera settings of existing surveillance cameras will not be moved, altered, or changed without the written approval of the Division Chief or facility administrator.
3. Administrators are responsible for ensuring maintenance of the camera surveillance system. Department employees or contracted companies may conduct maintenance.

C. Surveillance

1. Employees may monitor live video for building security and offender movement and behavior.
2. Division Chiefs and facility administrators will identify positions with the ability to live monitor remotely from a desktop.
3. Division Chiefs and facility administrators will identify staff positions with authority to retrieve recorded video images to review incidents and assess potential problems impacting security.
   a. These staff positions may show recorded video images to employees for the following reasons:
      1) pre-approved training; or
      2) an immediate security need, such as staff assisting with identifying offenders in an incident.
4. Employees may only view recorded video images if a legitimate business-related need exists.
5. Employees may not view recorded video images of any incidents that may have potential for criminal prosecution, staff discipline, or involving staff or offender injury for safety related investigation purposes unless written approval has been given by the facility administrator or Investigations.

D. Access

1. The following positions have the authority, within the scope of their position, to allow or block access to Department surveillance camera systems:
   a. the Director and Deputy Director;
   b. the Chief General Counsel;
   c. the Investigations Bureau Chief;
   d. the Department PREA Coordinator;
   e. the Information Technology CIO; or
   f. the Division Chief or facility administrator.
2. The level of access for each employee designated and approved by the above individuals must be identified, including whether the individual is allowed to view, save, copy, store, or delete video images.

E. Record Retention

1. Video images captured on Department surveillance cameras will be copied, saved, and/or stored only on approved and physically secure Department devices such as a server, desktop computer, mobile computing device or media, and only when approved by:
   a. the Director or Deputy Director;
   b. the Chief General Counsel;
   c. the Investigations Bureau Chief;
   d. the Department PREA Coordinator;
   e. the Information Technology CIO;
   f. the Division Chief or facility administrator; or
   g. any of these individual's designees.
2. All video images reviewed as part of an official investigation or official administrative process, including but not limited to use of force reviews, inmate disciplinary process, PREA investigations, and employee discipline, will be:
   a. noted or referenced, even if not relied upon, in the investigative or administrative record or report; and
   b. copied, saved, and/or stored and retained as part of the investigative or administrative record.

3. When video images captured by surveillance cameras are part of any matter being litigated or a hold is issued for video images, the video images will not be destroyed and will be retained until released by Department Legal Services.
4. Video images that are not reviewed or copied, saved, and/or stored will be retained for a minimum of time as determined by the system's storage capabilities.

V. CLOSING

Questions about this policy should be directed to the appropriate administrator.

VI. REFERENCES

A. *53-1-203, MCA*
B. *DOC 1.1.17 Prison Rape Elimination Act (PREA)*