STATE OF MONTANA
DEPARTMENT OF CORRECTIONS
POLICY DIRECTIVE

Policy No.: DOC 3.1.27	Subject: **CAMERA SURVEILLANCE SYSTEM**
Chapter 3: FACILITY/PROGRAM OPERATIONS	Page 1 of 3
Section 1: Security Operations	Effective Date: 04/28/2017
Signature: /s/ Loraine Wodnik, Interim Director	Revised:

I. POLICY

The Department of Corrections 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

Mobile Computing Device – Includes a laptop computer, tablet computer, smartphone or any device that performs similar functions and may or may not connect to a department network.

IV. DEPARTMENT DIRECTIVES

A. General Guidelines

1. Surveillance cameras are used in Department facilities, offices, and other buildings to ensure safe, secure, and humane operations. They will only be used by authorized individuals and only for approved Department business purposes.

2. Division and facility administrators are responsible for managing camera surveillance systems in accordance with this policy.

3. In accordance with *DOC Policy 1.1.17 Prison Rape Elimination Act of 2003 (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. This consideration will be documented in writing and forwarded to 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 the 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 Division Administrator, 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 or facility administrator, or designee.

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 to monitor building security and offender movement and behavior.

2. Division and facility administrators will identify positions with the ability to live monitor remotely from a desktop.

3. Division and facility administrators will identify staff positions with authority to retrieve recorded video images to review incidents and assess potential problems impacting security. These individuals may show recorded video images to employees for the following reasons:
   a. pre-approved training; or
   b. an immediate security need, such as staff assisting with identifying offenders in an incident.

4. Employees may only view recorded video images if 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 administrator, or designee, or the Office of 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 Legal Counsel;
   c. the Chief of Investigations;
   d. the Department PREA Coordinator;
   e. the Information Technology Division Administrator; or
   f. the division or facility administrator.

2. The level of access for each employee designated and approved by these individuals must be identified, including if 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/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 Legal Counsel;
   c. the Chief of Investigations;
   d. the Department PREA Coordinator;
   e. the Information Technology Division Administrator;
   f. the division 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/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 the Department's Legal Services.

4. Video images that are not reviewed or copied/saved/stored will be retained for a minimum of amount of time as determined by the system's storage capabilities.

V. CLOSING

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

VI. REFERENCES

A. 53-1-203, MCA
B. DOC Policy 1.1.17, Prison Rape Elimination Act of 2003 (PREA)

VII. ATTACHMENTS

None