
POLICY NAME:	Public Cameras and Centralized Video System
POLICY NUMBER:	20-P04
BOARD APPROVAL DATE:	May XX, 2020

1. GENERAL INFORMATION

This policy addresses public cameras and centralized video storage within the County of Lassen Internet Protocol Network (County Network). Applicable cameras are located in areas frequented by the public and/or common employee areas. Data storage is centrally managed by the Information Services Department (ISD). The course of operational viewing of the camera feed(s) is determined by departmental need. The purpose of the system is to enhance employee security and protect County assets.

IP video cameras are positioned at various County locations. Some live camera feeds are available to approved departments or employees, per the approval process outlined in this policy. The approved camera feeds are then rendered to a single computer monitor or to a video wall or larger display. Signage indicating the use of video must accompany any public camera installations.

Any enterprise-level video management system software (VMS) provides for customization of the camera feeds to any connected display. ISD provides this support by installing the VMS application and supporting its use.

ISD maintains control at the account level for individual or group access to specific cameras or groups of cameras. The Department Head makes the request for the individual or group access; approval is made by the County Administrative Officer (CAO).

Recorded data, qualifying as Non-Judicial Video Systems, is subject to disclosure pursuant to the Public Records Act (California Government Code Section 6250 et. seq.). There is no expectation of privacy where cameras within the system are positioned. ISD will assist with providing approved release of records.

2. DEFINITIONS

- Operational viewing (video surveillance) is the act of employees viewing live camera feeds during the course of their normal duties.
- Non-Judicial Video Systems are cameras and data storage systems within The County which are not legislatively mandated for minimum retention of 365 + 1 day.
- IP Video Cameras are those capable of recording and are connected to the County's IP network and managed by ISD.
- Account Level Control is employee access to County computer systems. Individual refers to a person. Group access is where viewing a display with camera feeds is located in a group work environment.
- Selective Video Release is the result of providing a video file or files to the requesting party. It is generally in response to the public records request (PRR) or to review security events such as unauthorized access, acts of vandalism, theft or other related incidents.

3. DEPARTMENTAL REQUESTS FOR VIDEO SURVEILLANCE ACCESS

The process for requesting access goes as follows:

- Department Heads request the camera feed(s) and those employees or groups to have access.
- Director of Personnel/CAO approves or denies the request.
- If approved, ISD creates the view and assigns the rights to the individual or group and installs the VMS application on the appropriate computer(s).

4. INSTALLATION OF PUBLIC CAMERAS GOVERNED BY THIS POLICY

Any new installation of public cameras must be approved by the CAO. The following are the minimum requirements for new installation requests.

- Requests must be made in writing or email;

- Define the camera(s) purpose and positioning;
- Describe any fiscal impact;
- If located within a specific department, departmental policy governing its use must be in place prior to the installation;
- Request is to be documented in the ISD ticketing system, known generally as helpdesk.
- Cameras governed by this policy may not have associated microphones. There is currently no audio component to this policy and installation of such companion devices is prohibited.

5. UNAUTHORIZED/PROHIBITED USE OF THE CAMERA SYSTEM

Lassen County (County) Employee conduct must meet the highest ethical standards. County employees, contractors, interns, volunteers, and others have legal responsibilities per HIPPA or IRS Guidance. Disciplinary procedures may be initiated for unauthorized or inappropriate use of video surveillance and/or the camera system. Any employee who engages in the unauthorized use of the camera system is subject to disciplinary action.

EXAMPLES OF UNAUTHORIZED/PROHIBITED USE

Providing selectively released footage without appropriate authorization or to unauthorized persons is prohibited. Other examples include:

- Discussing the contents of selectively released footage to unauthorized persons.
- Taking photos or video of selectively released footage from a personal camera or cell phone, or other device.
- Releasing non-redacted selective video which contains personal health information (PHI), personally identifiable information (PII), federal taxpayer information (FTI), or other protected information classifications.

6. PUBLIC RECORDS REQUEST (PRR)

The following describes how PRR are administered:

- ISD receives requests from Department Head with approval to proceed by the Office of County Counsel (CCL).
- ISD distributes the footage via agreed medium—file transfer, USB storage, optical disk, etc. The Requestor must provide the media and is responsible for delivering raw media and picking up the completed copy of the record. The requestor provides a usable shipping account number if the record(s) require shipping.

7. DEPARTMENTAL REQUESTS FOR SELECTIVE VIDEO RELEASE

Department Heads request the selective video release.

- Director of Personnel/CAO approves or denies the request.
- If approved, ISD will transfer the data securely to an appropriate location on the network or to media provided by the requester.
- Prior to releasing the video, it must be reviewed with a designated member of the requesting department to perform final review. This protection is in place to prevent the release of PHI, PII, FTI, or any other data which, if improperly released, could warrant sanctions against the County or individual.

8. ADMINISTRATIVE REQUESTS FOR SELECTIVE VIDEO RELEASE

The Personnel Director/CAO or Office of County Counsel have full authority regarding selective video release to investigate any incidents.

A. FILE SIZE AND DATA TRANSFER

Due to the size of video files, ISD may need to transfer the approved selective video release in a piecemeal fashion. Placing to department drives or H: drives may place too much strain on operational resources. In many cases, transferring the data to requesting party's primary work computer may be practical. Members of the public or other stakeholders outside of the Network with approved requests must provide the suitable media to enable the data transfer.

9. DATA RETENTION

ISD shall maintain/retain the video files for a period not to exceed 60 days, unless an approved exception to the 60-day period applies. Up to or prior to the 60-day period, the stored video is replaced (recorded over) on a first in-first out (FIFO) methodology.

Selective video releases may be retained at the department level for longer periods of time pursuant to specific administrative/disciplinary or criminal investigation or proceeding regarding behavior or activity that appears to be unauthorized, improper, illegal, or in furtherance of illegal activity.

Video footage that is retained by any department for these purposes shall be destroyed no later than one year after the administrative/disciplinary or criminal investigation or proceeding has concluded, unless it is retained for training purposes or the law or County policy require a longer retention.

DRAFT