

UCI GUIDELINES FOR FACILITY INSTALLATION AND OPERATION OF SECURITY CAMERAS

June 2026

Purpose

The purpose of these guidelines is to regulate the use of Security Camera Systems (SCS) on University Property. The University must balance safety and security needs with privacy and legal concerns over audio and video recordings with security cameras.

Security Cameras are designed to enhance safety and security at UCI. They are primarily used as a tool to record incidents for later reference related to injuries, crimes, accidents, and/or property damage occurring on UCI property. Cameras are not routinely monitored, but can be accessed in response to alarms, developing events, or emergencies. Anyone considering installing security cameras in any space owned or controlled (i.e., leased by) the University is expected to follow these guidelines.

Scope

The scope of these guidelines applies to UC Irvine units requesting a new security camera system or updates to an existing security camera system on University Property. UCI Health may have different guidelines for healthcare settings and should be consulted when applicable.

This Policy scope is intended to cover Security Cameras and does not include cameras utilized for the following purposes:

- Delivery of Education and Training Programs;
- Medical Procedures or Diagnostics;
- Research Activities – under an approved protocol;
- Artistic Performances, Athletic Events;
- Video Conferencing;
- Use by Law Enforcement, Event Management Team, or Emergency Management;
- License Plate Readers or documentation of illegal parking by TDS;
- Commercial Filming approved under Filming on Campus Policy;
- Use of personal cameras on phones and other devices (eye ware) not used for commercial purposes and otherwise compliant with laws, policies and regulations; or
- Time Lapse or cameras used to document construction or other for historical reference.

All camera use on campus must be done according to applicable laws, regulations, and policies.

Installation of a New or Replacement SCS

All new or replacement installations of security cameras shall comply with the following rules:

- a. Facilities Management (Security Program Manager) or designee - shall be consulted prior to the installation of any new video surveillance system. They will help to coordinate with other offices to ensure guidelines are followed. This contact is currently James Layne (Jlayne@uci.edu) X41308

INSTALLATION STANDARDS

1. Installation Compliance

All installations must comply with:

- California Building Code
- California Fire Code
- California Electrical Code
- UC Seismic Design Requirements
- UCI Facilities Design Standards
- ADA clearance requirements

2. Prohibited Installation Locations

Security cameras may not be installed in:

- Restrooms
- Shower Areas
- Locker Rooms
- Changing Facilities
- Lactation Rooms
- Residential Sleeping Quarters
- Private Offices without documented justification
- Any other area where there is a reasonable expectation of privacy

3. Applicable Legal and Regulatory Framework

Any questions regarding legal and regulatory requirements should be directed to the UCI Office of Campus Counsel.

Union Requirements

HR Labor Relations should be consulted when areas being recorded focus on represented staff. Notice to the Unions may be required in certain circumstances.

California Law

- California Constitution Article I, Section 1 (Right to Privacy)
- California Penal Code Section 632 (Audio recording restrictions)

Federal Constitutional Considerations (Public Institutions)

- *Katz v. United States*, 389 U.S. 347 (1967)
- *O'Connor v. Ortega*, 480 U.S. 709 (1987)

4. Field of View & Privacy Buffer Requirements

Facilities must evaluate over capture into adjacent private areas, viewing angles into residential facilities, and capture of neighboring non-UC property.

5. Audio Configuration

Audio functionality must be disabled at installation unless written authorization from Campus Counsel is provided.

6. Infrastructure & Cyber Coordination

Facilities Management shall coordinate with UCI Police Department and Office of Information Technology regarding access and storage of SCS video.

Secure Passwords and servers shall be used as determined feasible by OIT.

Units or personnel shall not install their own Security Camera Systems. Use of dummy cameras is not allowed. All installations Must utilize UCI Facilities Management following this protocol.

7. Privacy Impact Analysis

A Privacy Impact Analysis shall be conducted for high-risk installations by FM, UCIPD, and or the Privacy office.

High risk installations include installations where the camera is likely to capture footage that includes sensitive personal data such as PIN numbers, medical data, transactions involving medical care, crime reports, student housing facilities, and other areas where sensitive or controlled data exists.

Other privacy concerns may require in certain areas the posting of signage indicating that security cameras are in place.

8. Retention of Records

All video records under these guidelines shall be kept for a period not to exceed the University of California Retention Schedule ([schedule](#)). As described under Function: 07. Public Safety Records.

Records may only be kept until the administrative use ceases. This generally is considered a period of no longer than 60 days unless a crime or other event is captured that shall require a longer period as described in the retention schedule.

9. Access and Disclosure of Video Records

Permission from UCIPD, or the VCA or Sr. AVC of DFA is required to access video recordings. Access is for internal UC business needs.

Any disclosure of video records to an outside party shall be routed through the UCI PRA office for determination of disclosure requirements. If such disclosure is required by legal process as may be required by a court of competent jurisdiction such as a warrant or subpoena, UCI legal shall be consulted.

Most video records are a matter of public record.

10. Annual Review

These guidelines shall subject to an annual review by Facilities Management, UCIPD, and the UCI Privacy Office.

11. Disagreement between Parties

Any disagreement between units as to the applicability, use, or meaning of these rules should first be discussed between the parties for resolution. In the event of an impasse, the matter will be brought to the Vice Chancellor, Finance and Administration, who will have the final word.