UCLA Interim Policy 133: Security Camera Systems

Issuing Officer: Administrative Vice Chancellor
Responsible Department: Administration
Effective Date: August 9, 2019
Supersedes: New

I. PURPOSE & SCOPE

UCLA is committed to protecting the quality of life of the campus community by integrating safety and security technologies consistent with industry best practices. A critical component of a comprehensive safety program is the use of Security Camera Systems (SCS).The use of SCS on University Property is intended to deter crime, aid in the apprehension of suspects, and enhance the overall safety and security of property and individuals of the campus community.

To ensure the protection of individual privacy rights in accordance with the core values of the University of California ("University"), the UCLA Principles of Community, and State and federal laws, this Policy addresses the use of SCS to meet the safety and security needs of UCLA, while respecting and preserving reasonable expectations of individual privacy.

The purpose of this Policy is to regulate the use of SCS on University Property and formalize the procedures to request a new SCS, update an existing SCS, and request an individual to become an SCS Operator. Additionally, this Policy outlines the requirements for recording, handling, viewing, retaining, disseminating, and destroying live and recorded SCS Images.

This Policy regulates the use of SCS but should not be construed as a directive or guarantee that SCS will be monitored in real time, twenty-four (24) hours per day, and seven (7) days per week.

This Policy applies to UCLA units requesting a new or updates to an existing SCS on University Property, regardless of system ownership or the affiliation of the owner within the University.

This Policy does not address Cameras when used for the following purposes:

- delivery of education/training;
- research activities, such as the monitoring of experiments or animal behavior;
- medical procedures;
- artistic or creative performances;
- athletic events;
- business/promotional production;
- commercial television or movie production (see UCLA Policy 863);
- personal mobile recording devices;
- video conferencing;
- automated license plate readers (see UCLA Policy 134);

- drone or other aircraft cameras (see UC Drone Policy);
- mobile recording device used during the course of law enforcement, parking enforcement or transportation operations; and
- law enforcement activity covered by other applicable federal or State laws, or University policies.

Cameras used for any purpose not explicitly excluded by this Policy must comply with this Policy. Clarification of this Policy should be directed to the Administrative Vice Chancellor.

II. DEFINITIONS

For the purposes of this Policy:

Camera refers to any digital, analog, or other device that captures Images, including but not limited to video cameras, cell phones and other similar mobile devices, webcams, and portable computing devices used for the safety and security of people and property.

Designated Campus Authority (DCA) is the individual or group designated by the Administrative Vice Chancellor with responsibility for reviewing and approving aspects of the SCS as set forth in this Policy.

Image refers to a depiction or likeness captured or recorded in a single frame (still, snapshot, photograph); a sequence of multiple, single frames shot over a period of time (stop action, time lapse); or multiple frames that form a moving picture (motion, film, video).

Operator is the individual who has been approved by the DCA to install, manage, operate, and/or use the SCS and/or have access to SCS recorded Images, potentially including but not limited to computer system administrators, security software administrators, installation technicians, and law enforcement officers.

Organization Head refers to one of the following: Vice Chancellor; Vice Provost; Dean; University Librarian; Director, Intercollegiate Athletics; Executive Director, ASUCLA.

Preservation refers to the process of securely storing and maintaining SCS Images to prevent their loss or destruction.

Security Camera Systems (SCS) refer to the individual Cameras, recorded Images, and any system that is used to manage, maintain, store, or control access of individual Cameras and/or recorded Images.

University Property refers to a) all University property operated as part of the UCLA campus, including campus buildings, structures and facilities, parking structures and surface lots, and grounds areas; and b) all off-campus University owned or leased property or facilities operated by UCLA.

III. POLICY STATEMENT

A. UCLA strives to provide a safe and secure environment while avoiding unnecessary intrusions upon academic freedoms or individual civil liberties, including but not limited to privacy, freedom of expression, and right of peaceful assembly.

B. SCS may only be deployed in locations where it is determined that its use will enhance the security and safety of either individuals or property without violating the reasonable expectation of privacy as defined by UC Policy or law.

C. The installation, administration, and operation of SCS on University Property, will comply with all applicable State and federal laws, University policies, and UCLA campus policies and procedures.

D. The DCA coordinates the management of all SCS, including installation, administration, and operation. SCS will not operate outside of the centralized management system without prior written approval from the DCA. Such exceptions will be granted rarely and only in unusual circumstances in which an independent management system is in the best interest of campus safety and security as determined by the DCA. In such circumstances, the operations of the independent system must still comply with other provisions of this Policy.

E. Under the direction of the DCA, Campus Technical Support or UCLA Health Technical Support, as applicable, will assist UCLA units with the installation and operation of SCS, consistent with this Policy.

F. UCLA units requesting a new SCS must comply with this Policy. Existing SCS must comply with this Policy no later than December 31, 2020, unless a written waiver has been issued by the DCA. In January 2021, unapproved or nonconforming SCS must be removed unless a written waiver has been issued by the DCA, permitting the continued use of the noncompliant SCS until a specific date at which time the SCS will become compliant or be removed.

G. The use of non-functional SCS (decoy, fake or "dummy" Camera) or hidden SCS are prohibited, unless written permission has been issued by the DCA in consultation with UCLA Police.

IV. PROCEDURES

The following procedures set forth the processes related to SCS requests and outlines the requirements for recording, handling, viewing, retaining, disseminating, and destroying live and recorded SCS Images. Any questions or concerns regarding the deployment or operation of SCS should be addressed to the DCA.

A. SCS Use Requests

The DCA reviews and approves or denies all SCS use requests, including new SCS and updates to existing SCS.

1. **Submit Request**. Prior to deploying a new SCS or altering or updating an existing SCS, the requesting unit is responsible for obtaining the Organization Head's approval, completing the required form(s) and documentation, and submitting the request online at https://police.ucla.edu/services/campus-security-cameras.
   The replacement of existing, approved SCS equipment does not require approval from the DCA if such replacement does not have potential privacy implications (e.g., changes in how digitized information is reviewed or used, changes in the nature of the physical space where someone has the expectation of personal privacy, changes in location or field of view of Camera, etc.).

2. **Exceptions.** Exceptions to completing an online request (see https://police.ucla.edu/services/campus-security-cameras) or any required information may be made in the event of an imminent threat to the safety and security of the campus community, but then only as outlined in this Policy. In such circumstances, all reasonable efforts will be made to obtain oral or written approval from the DCA, prior to deployment of SCS. If oral approval was obtained, written approval must be obtained as soon as possible thereafter, but no later than two business days after deployment. If subsequent approval is not obtained within the time specified above, SCS must be decommissioned.

3. **SCS Inventory.** The DCA will maintain a master inventory of all SCS and will review system inventories at least annually. Campus Technical Support or UCLA Health Technical Support, as appropriate, will aid in the review, which may be performed by evaluating paper documentation (audit), physical inspection, or any combination thereof.

B. SCS Operator Requests

The DCA reviews and approves or denies all requests for individuals to become an Operator and will review Operator access privileges no less than annually.

1. **Submit Request**. Prior to use or access to the recorded Images of the SCS, the requesting unit is responsible for obtaining the Organization Head's approval, completing the required form and documentation, and submitting the request online at https://police.ucla.edu/services/campus-security cameras.
2. **Exceptions**. See section IV.A.2.

3. **Criteria for SCS Operators**. SCS Operators will be limited to individuals who meet and will continue to meet the following:
   a. have a justifiable need for access consistent with the purposes of this Policy;
   b. pass a background check as defined by the DCA, which may have stricter requirements than UCLA Human Resources Procedure 21 - Appointment;
   c. are appropriately trained and supervised in the technical, responsible, effective, legal, and ethical use of SCS;
   d. provide written acknowledgement that they have read, understand, and will comply with this Policy;
   e. perform their duties, including access to live or recorded Images, strictly as authorized by the DCA and in accordance with this Policy.
4. **SCS Operator List**. The DCA will maintain a list of authorized Operators, including who may be contacted about access to SCS after business hours. Campus units must alert the DCA as soon as possible regarding changes to contact information.

C. SCS Use Requirements

The use of SCS are limited to the purpose of enhancing campus safety and security, including crime prevention, law enforcement, and compliance with University policies. SCS will not be accessed or used for any other purpose except as outlined in this Policy.

Although the physical configurations of SCS may vary by location and may include monitoring via live feed or recorded Images, the functions of these systems fall into two main categories:

- **Property Protection:** Where the main intent is to aid in the apprehension of suspects when property is reported stolen, damaged, or vandalized.
- **Personal and Work Place Safety**: Where the main intent is to aid in the investigation of an incident in which someone's personal safety may be compromised.

Once the DCA has approved the use of a new or updates to an existing SCS, the UCLA unit will coordinate with the Campus Technical Support or UCLA Health Technical Support, as appropriate, on the installation, administration, and operation of the SCS in accordance with the following SCS use requirements:

1. **Equipment Specifications and Maintenance**. All SCS acquired after the effective date of this Policy through purchase or by any other means must comply with the technological and other specifications as determined and set forth by the DCA in consultation with Campus Technical Support or UCLA Health Technical Support, as appropriate, and UCLA Information Technology Services (ITS), in accordance with but not limited to the UCLA Campus Security Camera Technical Standards Guidelines.

   SCS equipment specifications include, but are not limited to, the following:

   - All cabling for SCS will be installed in compliance with current ITS guidelines.
   - Each SCS must have a maintenance plan including, but not limited to, 1) dome-cleaning schedule, 2) regular camera image audits to ensure good image quality; 3) a process to address the repair and replacement of inoperable SCS equipment, including poor image quality and weak or lost signals and pan, tilt, zoom (PTZ) functionality; and 4) a lifecycle replacement schedule.
2. **Signage and Posted Notice.** In accordance with any applicable federal, State, local laws and University policies, including the Electronic Communications Policy and the University Statement of Privacy Values and Privacy Principles, signage will be posted at building entrances or other areas where SCS have been deployed, indicating that the area is being monitored or recorded. Prior to posting signage, all signage must be reviewed by the Campus Architect.

Standard posted signage should read:

"Security Cameras on Premises"

For more information, contact UCLA Police at (310) 825-1491."

Questions or concerns regarding the content or location of signage should be directed to the DCA.

3. **Monitoring.** SCS monitoring will comply with the following:
   a. The monitoring of individuals or groups of individuals through SCS via live feed or recorded Images will be based on current or prior explicitly exhibited behaviors that potentially violate law or University policy and such monitoring must be conducted in a manner consistent with applicable University and local campus policies, and State and federal laws.

   b. Under normal operating conditions, SCS not intended to be actively monitored may be monitored for legitimate safety and security purposes, that include but are not limited to the following: areas in which an alarm has been triggered; areas identified as high risk due to existing safety or security concerns; restricted access areas; areas in which special events are occurring; and areas under specific investigations authorized by the Chief of Police or designee.

   c. While monitoring live feed Images, an Operator may notify UCPD of violations of law or UC Policy impacting the safety and security of the campus community.

4. **Access**. Access to SCS live feed or recorded Images is limited to authorized Operators and persons authorized by the Vice Chancellor of Legal Affairs, Administrative Vice Chancellor, Vice Chancellor for Health Sciences, or the Chief of Police. A record log will be kept by the DCA of all individuals with access to and use of live feed or recorded Images.

   This section is not intended to limit the authority of UCLA Police in law enforcement activities. Upon request by the DCA, UCLA Police or UCLA Legal Affairs, campus units must provide immediate and unrestricted access to live and recorded Images obtained using legacy stand-alone SCS. Additionally, legacy stand-alone systems without network capabilities will be phased out before 2020, unless written exception is granted by the DCA.

5. **Unauthorized Access.** Any unauthorized access to SCS, including the inadequate protection, inappropriate use, disclosure, or disposal of live or recorded Images must be reported immediately to the DCA and subsequently reported and notifications issued as required by relevant cyber security policies, including but not limited to UCLA Policy 420: Breaches of Computerized Personal Information and BFB-IS-3: Electronic Information Security Policy.

6. **Prohibited Use.** SCS will not be used for the following purposes:
   - audio recording associated with a video Image is prohibited except when explicit notice has been given to those being recorded and specifically approved by the Vice Chancellor for Legal Affairs in connection with a civil investigation, or directed by a specific court order.
   - targeted recording or monitoring of individuals based solely on personal characteristics, including age, color, disability, gender, national origin, race, religion, sexual orientation, or other federal or State protected characteristics;
   - to monitor or record sensitive institutional or personal information (e.g., medical records, personnel records, etc.);
   - to monitor or record spaces in which individuals have a reasonable expectation of privacy, including, personal offices, personal living spaces, unless required and specifically approved by the Chief of Police in connection with a criminal investigation, approved by the Vice Chancellor for Legal Affairs in connection with a civil investigation, or directed by a specific court order.

D. Operator Use Requirements

Once the DCA has approved the SCS Operator, the Operator must comply with the following Operator use requirements:

1. **Access.** An authorized Operator may access the SCS in accordance with the type of access approved by the DCA (See https://police.ucla.edu/services/campus-security-cameras) and this access may include the monitoring and/or review of live feed or recorded Images, solely for the following purposes:

   a. maintenance of SCS equipment or systems;

   b. investigation of suspected illegal criminal activity;

   c. investigation of suspected activities in violation of University policy;

   d. compliance with legal obligations to preserve, release, or otherwise use live feed or recorded Images; and

   e. general safety and security monitoring consistent with the intent of this Policy.

   SCS Operators with authorization to review live or recorded Images must be provided appropriate work areas in which said review can be conducted privately to prevent unauthorized individuals from inadvertent, advertent, unintentional, or intentional access. SCS will provide for individual authenticated user access and logging of user activity consistent with UCLA information systems security standards.

2. **Prohibited Use**. In addition to the prohibited use of the SCS as stated in section IV.C.6 of this Policy, Operators are also expressly prohibited from:

   a. duplicating recorded Images for any purpose not permitted by Policy;

   b. permitting or providing access to live or recorded Images to anyone not specifically authorized by the DCA;

   c. operating or using SCS outside the scope of the usage approved by the DCA; and

   d. viewing, recording, accessing or otherwise using SCS in any manner that is inconsistent with this Policy or any other safeguards deemed appropriate by the DCA.

E. Recorded Images

1. **Storage and Retention of Recorded Images.** Any recorded Images obtained and retained through SCS will be stored and secured as required by ITS to ensure appropriate security protocols are followed and to prevent unauthorized access, modification, duplication, or accidental destruction. Additionally, the storage of recorded Images will be consistent with the UCOP electronic data storage and cybersecurity policies.

   Recorded Images will be stored for a period of no less than thirty (30) days and no more than ninety (90) days, and then deleted or destroyed unless University policy defines a longer retention period (see UC Records Retention Schedule and UC BFB RMP-2 Records Retention Disposition) or one or both of the following conditions exist:

   a. The recorded Images are being retained by law enforcement as part of a criminal or civil investigation or court proceeding. Any such recorded Images copied and retained by law enforcement will be retained and secured in accordance with applicable evidence laws and campus policies and no longer subject to this Policy's requirements.

   b. A written directive to retain the recorded Images for a specified period of time has been issued by the Vice Chancellor of Legal Affairs, Administrative Vice Chancellor, Vice Chancellor for Health Sciences, Vice Chancellor of Student Affairs, Vice Chancellor for Equity Diversity and Inclusion, Director of Insurance and Risk Management, the Chancellor, or the Executive Vice Chancellor and Provost. A copy of the written directive must be immediately provided to both the DCA and the

Vice Chancellor of Legal Affairs. The DCA will retain the written directive and ensure the Preservation of recorded Images.

Such a written directive may occur for any of the following reasons:

i. upon receiving credible notification of a University or law enforcement investigation for alleged illegal activity or violations of University policy;

ii. upon receiving notice from Legal Affairs that such copying and storage is otherwise needed to comply with legal obligations to preserve materials;

iii. upon receiving authorization that such Preservation reasonably appears necessary to protect University operations;

iv. where there is a reasonable belief that the recorded information may relate to misconduct or violations of law or University policy; or

v. where the video information has historical significance (*e.g.*, building construction, natural or manmade disaster or other historically significant event).

2. **Public Release of Recorded Images.** All requests for the distribution of recorded Images must be submitted to the DCA. Formal California Public Records Act requests should be processed in coordination with the UCLA Records Management and Information Practices Office. The DCA receives, documents, and retains each request for and determination regarding the release of SCS recorded Images and may consult with Legal Affairs, UCLA PD, Campus Privacy Officer, or Campus Human Resources as applicable and appropriate. Upon a showing of a legitimate need consistent with the purposes of this Policy, the DCA may permit the distribution of recorded Images under one or more of the following circumstances:

a. Significant Public Interest: The recorded Images depict or document conditions or activities that are public in nature and do not violate any individual's expectation of privacy, and are of significant importance to the general public (e.g. building construction, earthquake, traffic patterns, weather conditions).

b. Explicit Consent: If an individual(s) that is clearly depicted in the recorded Images provide(s) explicit consent to its distribution.

c. Legal Requirement: All requests to access recorded Images to satisfy a legal requirement (e.g., requests under the California Public Records Act, subpoenas, warrants, court orders and other legal documents) must be delivered immediately to UCLA Legal Affairs. No access will be granted without review and approval by Legal Affairs.

d. Law Enforcement Action: If an external law enforcement agency (e.g., FBI, Los Angeles PD) executes a search warrant or other order for immediate access or confiscation of recorded Images, SCS Operators should first seek approval from Legal Affairs or UCLA PD, and if not possible, document the actions of law enforcement officers, and notify both the DCA and Legal Affairs as soon as possible. Whenever possible, SCS Operators should take reasonable steps to document and preserve a copy of any recorded Images being removed.

e. Emergency Situation: In response to an emergency on campus when deemed to be necessary by the incident commander or other competent authority. Such use will be documented and reported to the DCA as soon as possible.

f. Incident Investigation: Distribution of the recorded Images are necessary to investigate or adjudicate a claim against UCLA.

Once the purpose for distribution has been satisfied, any copied Images provided, will, to the extent possible, be deleted or destroyed in a manner consistent with current ITS protocol, documented, and reported to the DCA.

3. **Deletion or Destruction of Recorded Images**. The deletion or destruction of recorded Images will be accomplished using a product or products that have erase or wiping capabilities that meet or exceed ITS guidelines and protocols. The DCA must be notified when recorded Images have been deleted or destroyed outside the parameters defined in section IV.E.1.

F. Appeals Process

Requests to review decisions made by the DCA should be submitted in writing to the Administrative Vice Chancellor within thirty (30) days of said decision. The Administrative Vice Chancellor will review the DCA's findings and issue a final determination either upholding the DCA decision or directing the DCA how to proceed.

G. Compliance Audit

The UCLA Audit and Advisory Services may audit and inspect all processes and records pertaining to the SCS, including a review of services and functions performed by the DCA, Campus Technical Support, UCLA Health Technical Support, Operators, and others with responsibilities as designated in this Policy and to confirm SCS have been deployed, operated, and maintained in compliance with this Policy.

H. Non-Compliance

Individuals who fail to comply with this Policy may be subject to disciplinary action under University policies or, as applicable, collective bargaining agreements (up to and including immediate termination of employment, student suspension, etc.), and/or criminal penalties under law.

Campus units, including but not limited to professional schools, departments, laboratories and other programs, that do not comply with this Policy are required to remove non-compliant SCS.

V. RESPONSIBILITIES

The following campus offices and officials have specific responsibilities with respect to the processes set out in this Policy.

RESPONSIBILITY	ACTION
Administrative Vice Chancellor	Oversees the management of the contents and the enforcement of this Policy.
	Appoints the DCA. The DCA will not approve or have final DCA decision-making authority over SCS under its direct control. An alternative method approved by the Administrative Vice Chancellorwill be used for these SCS.
	Hears appeals of DCA decisions.
	Appoints staff to oversee Campus and Health System technical support.
Designated Campus Authority (DCA)	Reviews and approves or denies requests to deploy and operate SCS in and around UCLA Property in spaces that do not violate the reasonable expectation of privacy as defined by law.
	Coordinates, as needed, with UCLA Police, Information Technology Services, Insurance and Risk Management, Chief Privacy Officer, Capital Programs, Facilities Management, Purchasing, and campus Legal Affairs to review proposals for the deployment and use of SCS.
	Coordinates, as needed, with Campus Technical Support and Health System Technical Support to ensure that deployment of SCS is consistent with industry best practices, complies with all federal and State laws, and is in accordance with the core values of the University and the UCLA Principles of Community.
	Monitors, reviews, and responds to concerns regarding the deployment and use of SCS.
	Monitors and inspects SCS to ensure compliance with this Policy.
	Issues waivers as appropriate to grant exceptions to this Policy, including the continued use of noncompliant SCS after December 31, 2020, and the use of decoy or hidden SCS.

Designated Campus Authority (con't)	Maintains an inventory of all SCS, including Camera locations.
	Reviews and approves or denies requests for proposed Operators. Maintains a list of authorized Operators and other users, including the Operators that may be contacted about SCS after business hours. Oversees the training provided to Operators, including appropriate resource and reference materials.
	Directs the removal of noncompliant SCS.
Campus Technical Support	Coordinates, as needed, with the DCA, UCLA Police, and Information Technology Services to provide technical support in the installation, maintenance, and management of campus SCS.
	Aids in the annual review of SCS and maintenance of campus system inventories.
Health System Technical Support	Coordinates, as needed, with the DCA, UCLA Police, UCLA Health Administration, and Information Technology Services to provide technical support in the installation, maintenance, and management of Health System SCS.
	Aids in the annual review of SCS and maintenance of Health System inventories.
UCLA Police	Advises the DCA as to the appropriateness of proposed SCS as a tool to increase security and that the full field of view of Camera conforms to this Policy.
	Advises the DCA as to the appropriateness of proposed decoy or hidden Cameras.
Insurance and Risk Management	Recommends to the DCA, SCS installation locations to reduce UCLA liability or loss of property.
Chief Privacy Officer	Recommends to the DCA, SCS installation locations that respects and preserves reasonable expectations of individual privacy.
Legal Affairs	Monitors developments in the law, industry practices, and technology pertaining to SCS.
	Advises the DCA as to the appropriateness and compliance of proposed SCS.
Organization Heads	Ensures SCS are managed within their area of responsibility and are compliant with this Policy.

VI. REFERENCES

1. California Public Records Act
2. UCLA Principles of Community
3. Electronic Communications Policy, University of California, 2005.
4. UCLA Policy & Procedures 420: Breaches of Computerized Personal Information
5. BFB-IS-3: Electronic Information Security Policy
6. UC Business and Finance Bulletin IS-3 Electronic Information Security
7. UC Records Retention Schedule
8. UC BFB RMP-2 Records Disposition Program and Procedures
9. UCLA Campus Security Camera Technical Standards Guidelines
10. Health Insurance Portability and Accountability Act (HIPAA)

Issuing Officer

/s/ Michael J. Beck

Administrative Vice Chancellor