UCLA Policy 133: Security Camera Systems
DRAFT for Public Review

Issuing Officer:	Administrative Vice Chancellor
Responsible Department:	Administration
Effective Date:	TBD
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) on the UCLA campus. The use of SCS on campus 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 approved SCS that are intended to enhance public safety and security on campus. Additionally, this Policy formalizes the procedures for requesting to deploy a new SCS and updates to an existing SCS, and outlines the requirements for recording, handling, viewing, retaining, disseminating, and destroying live and recorded SCS Images on campus.

This Policy applies to SCS that monitor or record Open Spaces at or within proximity to UCLA's Westwood campus, including South Campus, Wilshire Center, and other Facilities owned or controlled by the University in and around Westwood Village, regardless of system ownership or the affiliation of the owner within the University.

The existence of this Policy does not imply or guarantee and should not be construed to imply or guarantee that SCS will be monitored in real time, twenty-four (24) hours per day, seven (7) days per week.

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;

- commercial television or movie production (see UCLA Policy 863);
- mobile recording device used during the course of law enforcement, parking enforcement or transportation operations;
- personal mobile recording devices;
- business/promotional production;
- video conferencing;
- law enforcement activity covered by other applicable federal or State laws, or University policies; and
- drone or other aircraft cameras.

Any purpose not explicitly excluded by this Policy must comply with this Policy.

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.

Facilities refers to the buildings, grounds, and all points of public ingress and egress that are located within areas owned or controlled, via leases or other contractual arrangements by the University, and whose operations are controlled by the University. Facilities include but are not limited to offices, labs, classrooms, auditoriums, indoor and outdoor assembly areas, building exteriors, hallways, parking lots and structures, outdoor public areas, and common areas. Buildings, grounds, or other properties owned by the University, but whose operations are under the control and operation of a non-University related business, will not be considered Facilities under 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).

Open Space refers to any outdoor area that is generally open to the public, including but not limited to landscaped areas, courtyards, and pathways of ingress and egress. It also refers to indoor spaces generally considered public although they may have restricted access, including but not limted to building lobbies, hallways, and assembly areas.

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.

III. POLICY STATEMENT

A. UCLA strives to provide a safe and secure environment while avoiding unnecessary intrusions upon academic freedoms or individual civil liberties such as 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 law.

C. The design, installation, implementation, operation, use, management, and maintenance of SCS on campus will comply with all applicable State and federal laws, University policies, and UCLA campus policies and procedures, including but not limited to those laws and policies that recognize an individual's reasonable expectation of privacy and prohibit discrimination and harassment.

D. The DCA coordinates the management of all SCS, including installation, administration, and operation. SCS shall 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 the other provisions of this Policy.

E. UCLA units requesting the procurement, installation, and operation of new SCS must comply with the requirements and procedures outlined in 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.

F. The use of non-functional SCS (decoy, fake or "dummy" Camera) deliberately designed and positioned to mislead an individual into believing an area is being monitored may generate a false sense of security and are prohibited unless written permission has been issued by the DCA in consultation with UCLA Police.

IV. PROCEDURES

The following procedures set forth the process to request a new or changes to an existing SCS, including access to SCS recorded Images, and outlines the requirements for recording, handling, viewing, retaining, disseminating, and destroying live and recorded SCS Images on campus.

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 deployment and updates to existing SCS, in accordance with this Policy. The replacement of equipment of existing approved SCS do 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.).

1. **Submit Request.** Prior to deploying or using a new SCS or updates to an existing SCS, the requesting unit is responsible for obtaining the Organization Head's approval, completing the required form and documentation (Attachment A) and submitting the request to the Administrative Vice Chancellor's Office, who will forward to the DCA.
2. **Exceptions.** Exceptions to completing the request forms (Attachments A & B) 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 shall 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 existing and approved SCS and shall review system inventories at least annually. The review 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 to ensure only authorized individuals have access to the SCS.

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 (Attachment B) and submitting the request to the Administrative Vice Chancellor's Office, who will forward to the DCA.
2. **Exceptions**. See section IV.A.2.
3. **Criteria for SCS Operators**. SCS Operators shall be limited to individuals who meet and will continue to meet the following:
   a. demonstrate a legitimate need for access consistent with the purposes of this Policy;
   b. are appropriately trained and supervised in the technical, responsible, effective, legal, and ethical use of SCS as outlined in this Policy;
   c. pass a background check;
   d. provide written acknowledgement that they have read, understand, and will comply with this Policy;
   e. perform their duties in accordance with this Policy; and
   f. access live or recorded Images only to the extent authorized by the DCA and as permitted by 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 polices. SCS shall 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, the functions of these systems fall into three main categories:

a. **Property Protection:** Where the main intent is to capture and store SCS Images to aid in the apprehension of suspects when property is reported stolen, damaged, or vandalized.
b. **Personal and Work Place Safety**: Where the main intent is to capture and store SCS Images to aid in the investigation of an incident in which someone's personal safety may be compromised.
c. **Extended Responsibility**: Where the main intent is to provide real time Images of an Open Space which may or may not be recorded but that can be monitored by an Operator.

Once the DCA has approved the use of a new or updates to an existing SCS, the DCA will coordinate with the UCLA unit 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 UCLA Information Technology Services (ITS). 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 that includes 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, and local laws as well as University policies, including the Electronic Communications Policy and the University Statement of Privacy Values and Privacy Principles, signage shall 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 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 shall 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. SCS established to provide an extended responsibility (see section IV.C.) are monitored continuously. The live SCS Images may be monitored by Operators; however, any video Images recorded must comply with the storage and retention requirements in Section IV.E.
   c. 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: high risk areas; restricted access areas; areas in which an alarm has been triggered; areas in which special events are occurring; and areas under specific investigations authorized by the Chief of Police or designee.

4. **Access**. Access to SCS live feed or recorded Images is limited to authorized Operators and persons authorized by Vice Chancellor of Legal Affairs, Administrative Vice Chancellor, Vice Chancellor for Health Sciences, or the Chief of Police. A record log shall 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 shall 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 reported as required by UCLA Policy 420: Breaches of Computerized Personal Information.

6. **Prohibited Use.** SCS shall not be used for the following purposes:
   - audio recording associated with a video Image, except when explicit notice has been given to those being recorded;

- 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, dormitories or other 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 attachment B) 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; and
   d. compliance with legal obligations to preserve, release, or otherwise use live feed or recorded Images.
   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 shall 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 shall 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 shall be consistent with the UCOP electronic data storage and cybersecurity policies.

   Recorded Images shall 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 Disposition Program and Procedures) 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 shall 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 shall 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 Department. 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**. The individual(s) depicted in the recorded Images provide(s) explicit consent to its distribution.

c. **Legal Requirement**. All requests or demands for individuals 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 shall be granted to individuals 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 designated authority. Such use shall 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, shall, 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 shall 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's decision or directing the DCA how to proceed.

G. Compliance Audit

The UCLA Director of 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, 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

Failure to comply with this Policy may result in 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.

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 shall not approve or have final DCA decision-making authority over SCS under its direct control. An alternative method approved by the Administrative Vice Chancellor shall be used for these SCS.
	Hears appeals of DCA decisions and issues a final determination.
Designated Campus Authority (DCA)	Reviews and approves or denies requests to deploy and operate SCS in and around UCLA Open Spaces and Facilities.
	Coordinates, as needed, with UCLA Police, Information Technology Services, Insurance and Risk Management, Capital Programs, Facilities Management, Purchasing, and campus Legal Affairs to review proposals for the deployment and use of SCS.
	Ensures 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.

DCA (con't)	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, 2019, and the use of decoy SCS.
	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.
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 Cameras.
Insurance and Risk Management	Recommends to the DCA, SCS installation locations to reduce UCLA liability or loss of property.
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. UC Video Security/Safety Systems Policy
4. Electronic Communications Policy, University of California, 2005.
5. UCLA Policy & Procedures 420: Breaches of Computerized Personal Information
6. UC Business and Finance Bulletin IS-3 Electronic Information Security

VI. ATTACHMENTS

A. Request Form for Security Camera Systems

B. Request Form for Security Camera Systems Operators

Request Form for Security Camera Systems

In order to request a new or update to an existing Secrity Camera System (SCS), this form must be completed and submitted to the Administrative Vice Chancellor's Office, who will forward to the Designated Campus Authority (DCA). UCLA Policy 133, Security Camera Systems, describes under what circumstances a request for an SCS may be considered for approval. It is recommended that this Policy be read *before* completeing this form.

A. REQUESTER'S NAME, TITLE AND DEPARTMENT/UNIT

_____ _____

B. PURPOSE AND JUSTIFICATION FOR SCS

C. SCS DETAILS

Attach a detailed explanation of the SCS, this includes: the physical location of monitoring or recording equipment; camera(s) locations with a brief description of the space in which the monitoring will occur, typical uses of the space, and the activities likely to be monitored by the SCS; capabilities of the camera(s) (video, audio, pan, tilt, zoomed, etc.); IP address, if applicable; and an explanation of how recorded images will be stored, maintained and discarded.

D. PROPOSED OPERATORS – List the proposed Operators (see Attachment B for Operator Approval). If necessary, attach list.

E. MEASURES TO BE TAKEN TO MINIMIZE IMPACT ON PERSONAL PRIVACY

F. ORGANIZATION HEAD ACKNOWLEDGEMENT & SIGNATURE

I assert that the planned deployment of the SCS will comply with all applicable laws, regulations, UC policies and UCLA Policy 133.

_____ **Date**:_____

Signature of Organization Head – check appropriate box:

☐ Campus ☐ Health System and School of Medicine

G. DCA SIGNATURE

Does the DCA approve? ☐ Yes ☐ No

_____ **Date:**_____

Signature of DCA

H. COMPLETED FORM ROUTING

The DCA will retain a copy of the completed form and return the original copy to the requestor named above.

Request Form for SCS Operators

In order to request an individual to become an SCS operator, this form must be completed and submitted to the Adminisrative Vice Chancellor's Office, who will forward to the Designated Campus Authority (DCA). UCLA Policy 133, Security Camera Systems, describes under what circumstances a request for an authorized operator may be considered for approval. It is recommended that this Policy be read *before* completeing this form.

A. REQUESTOR'S NAME, TITLE AND DEPARTMENT/UNIT

_____ _____

B. PROPOSED OPERATORS

Attach an alphabetical list of proposed operators and include for each proposed operator the following information: the supervising unit's name and contact info; proposed Operator's full name, position, University ID, and contact information; the type of access being requested (e.g. computer system administrator, software administrator, installation technician, access to monitor or recorded images, etc.); list of SCS to which the proposed operator would have access to; any restrictions to the proposed Operator's access to live and recorded images; and the purpose and justification for the access.

C. PROPOSED OPERATORS ACKNOWLEDGEMENT

Attach the written acknowledgement of each proposed operator that they have read, understand, and will comply with all applicable laws, policies, and UCLA Policy 133.

D. ORGANIZATION HEAD SIGNATURE

_____ **Date:** _____

Signature of Organization Head

Signature of Organization Head – check appropriate box:

☐ Campus ☐ Health System and School of Medicine

E. SIGNATURE OF DCA

Does the DCA approve? ☐ Yes ☐ No

_____ **Date**:_____

Signature of DCA

F. COMPLETED FORM ROUTING

The DCA shall retain a copy of the completed form and return the original copy to the requestor named above.