UNIVERSITY OF CALIFORNIA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

EXECUTIVE VICE PRESIDENT — CHIEF OPERATING OFFICER

OFFICE OF THE PRESIDENT
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200
510/987-0500

June 22, 2017

PROVOST DORR
VICE PRESIDENT DUCKETT
VICE PRESIDENT HOLMES-SULLIVAN

Subject: Proposed Policy on Video Security/Safety Systems

Dear Colleagues:

The proposed *Policy on Video Security/Safety Systems* is ready for review and vetting by your respective processes and constituents. Please distribute the attached draft policy—as required by your internal processes—to these groups and ask them to review and provide any feedback to Chief of Staff Cathy O'Sullivan at cathy.osullivan@ucop.edu.

The policy was developed by a workgroup led by Systemwide Deputy Compliance Officer David Lane and comprised of a broad range of campus and UCOP partners including representatives from security, law enforcement, legal, compliance, privacy, academic personnel, student affairs, and human resources. The workgroup met over several months, developed several drafts, and received input from a variety of other campus groups such as campus policy managers. This final draft has been reviewed by the Office of the General Counsel.

Please let Cathy know if your office will be sending out this policy for campus and constituent vetting and, if so, how long that vetting process will take. That way, our office can track the comments and process so that we can finalize this policy in a timely fashion.

If you have any specific questions or need more information about the vetting process, please contact Cathy at (510) 987-0121. Thank you for your cooperation and assistance.

Sincerely,

Rachael Nava

Rachael Nava
Executive Vice President
Chief Operating Officer

Attachment

cc: Vice Provost Carlson
Deputy Griffin-Desta
Chief Policy Advisor Kao
Systemwide Deputy Compliance Officer Lane
Campus Policy Managers
Chief of Staff Henderson
Chief of Staff O'Sullivan

Video Security/Safety Systems

Responsible Officer:	EVP - Chief Operating Officer
Responsible Office:	BO - Chief Operating Officer
Issuance Date:	[Issuance Date]
Effective Date:	[Effective Date]
Last Review Date:	***Draft Version 12_3.6.2017***
Scope:	This Policy applies to all organizations or entities governed by the Regents of the University of California. This policy covers Video Security and Safety Systems.

Contact:	Cathy O'Sullivan
Title:	Chief of Staff to COO
Email:	Cathy.OSullivan@ucop.edu
Phone #:	(510) 987-0121

I. POLICY SUMMARY

The use of a Video Security/Safety System (VS/SS) is a means to help deter crime and to promote safety and security for people and property. This Policy addresses installation and use of VS/SS equipment at the University of California (University). It seeks to address public safety concerns while protecting individual rights and academic freedom.

II. DEFINITIONS

Dummy Camera – A decoy device deliberately designed and positioned to mislead an individual into believing an area is being monitored and/or recorded when it is not.

Executive Officer – The University President, Chancellor, Director of Lawrence Berkeley National Laboratory, or Vice President of Agricultural and Natural Resources

Location – All organizations or entities governed by the Regents of the University of California.

Private Spaces – Settings where an individual has a reasonable expectation of privacy and of being free from surveillance. This does not include a place where the general public has lawful access. Following are some examples of Private Spaces: residential living quarters, bathrooms, locker rooms and private offices. This list is not comprehensive refer to the list of Private Spaces as designated by each Location.

Public Areas – Indoor or outdoor spaces that are open and accessible to the general public and are not Private Spaces.

Sensitive Areas – Settings determined to be a high risk that require special protection. Following are some examples of Sensitive Areas: data centers, power facilities, facilities with secure requirements, any areas that store hazardous or controlled materials (i.e., pharmaceuticals, ethyl alcohol and chemicals used for research), museums and art galleries, hospitals, animal care facilities, and any areas in which the exchange of currency or other forms of payment occur. This list is not comprehensive refer to the list of Sensitive Areas as designated by each Location.

Video Data (VD) – Visual images recorded by a University VS/SS that can be replayed, stored and deleted.

Video Security/Safety System (VS/SS) – Any device, component or system that captures images to assist in promoting the security and safety of people and property at a Location.

III. POLICY TEXT

A. *General*

The University recognizes and respects protected individual freedoms, the preservation of individual privacy, freedom of expression and civil liberties of all persons accessing any Location. This Policy is intended to balance these freedoms with crime deterrence and the need to promote a safe and secure University environment. This Policy is consistent with the University Statement of Privacy Values and Privacy Principles which defines privacy as the ability of an individual to conduct activities without concern of observation as well as the standards for the appropriate protection, use and release of personal information.

Installation and operation of every VS/SS, must comply with federal, state and local laws as well as University policies. Targeted recording or monitoring of individuals based on characteristics such as race, color, disability, gender, gender identity, national origin, religion or other protected classifications is strictly prohibited.
Use of Video Data (VD) must be limited to safety, security and crime prevention purposes. VS/SS must not be used to view or record Private Spaces, unless required in connection with a criminal investigation or specific court order.

Decisions to install, upgrade or replace a VS/SS must be made in consultation with offices designated by each Location in accordance with this Policy and related local procedures as determined by the Executive Officer or designee(s). Any request for authorization must include a de-commission or removal date.

Personally owned cameras may not be installed or used as a VS/SS at any Location unless prior written authorization is granted by the Executive Officer or designee(s).

B. ***Scope***

This Policy does not apply to the use of VS/SS for law enforcement activities.

The following video applications are outside of the scope of this Policy:

- delivery of education/training;
- all uses for research purposes, including vivariums and biosafety labs;
- video recording medical procedures for quality assurance purposes;
- recording of artistic or creative performances;
- retail loss prevention operations;
- recording of athletic events;
- commercial television or movie recordings;
- any mobile recording device used during the course of law enforcement, parking enforcement or transportation operations; and
- use of personal recording devices unrelated to official UC business.

C. ***Placement of University VS/SS***

Typical placement of VS/SS equipment at a University Location includes, but is not limited to:

- building facades, elevators, stairwells, entrances and exits;
- public areas including parking facilities; and
- entry and exit points to any Sensitive Area.

VS/SS equipment must never be placed in Private Spaces or used for workforce monitoring or performance management of UC employees without approval by the Executive Officer or designee(s). In accordance with the University's Sexual Violence and Sexual Harassment policy the invasion of sexual privacy (Section B.3 of Prohibited Conduct) is strictly prohibited.

VS/SS equipment must be monitored to protect from tampering or disabling and must be operational. Use of any Dummy Camera is prohibited. Audio recordings are prohibited and any audio features of VS/SS equipment must be disabled.

D. ***Notification of VS/SS Use***

Conspicuous notification stating that a Public Area is being recorded must be made in accordance with federal, state and local laws as well as with UC policies, including the Electronic Communications Policy and the *University Statement of Privacy*

Values and Privacy Principles. Placement of signs accompanying VS/SS is determined by the Executive Officer, or designee(s).

E. ***Use of Video Data***

University employees managing VS/SS technology or with access to Video Data must be provided a copy of this Policy as well as related local procedures and must receive appropriate training on:

- operational use of VS/SS; and
- information on privacy and security implications of video recording.

Video recording must be conducted in a professional, ethical, and legal manner. Every review of Video Data must be conducted in a manner consistent with federal, state, and local laws and University Policy.

Any violations of law discovered via Video Data must be reported to the campus police department. Discovery of a prohibited activity by a student or an employee that may warrant disciplinary action must be reviewed and the proper action determined by the appropriate administrative offices such as the Office of General Counsel, Staff Human Resources, Academic Personnel, or Student Affairs.

Every request for access to Video Data must be submitted to the Executive Officer or designee(s). Each location will implement procedures for requesting and approving access to Video Data, including procedures for internal requesting parties, public records requestors, and in connection to legal action such as a lawfully issued subpoenas.

The VD from a VS/SS must be securely stored and maintained in accordance with the *UC Records Retention Schedule*, or at least 21 calendar days, whichever is longer. Destruction of VD will be in accordance with BFB-**RMP-2**: Records Retention and. Disposition: Principles, Processes, and. Guidelines.

IV. COMPLIANCE / RESPONSIBILITIES

A. ***Implementation of the Policy***

Executive Officers, or designee(s), must develop procedures and supplemental information to support the implementation of this Policy (refer to Section V. Procedures). The Responsible Officer, Office of the President, will apply appropriate and consistent interpretations of the Policy that do not result in substantive changes to this Policy.

B. ***Revisions to the Policy***

The President approves this Policy and any revisions. The Responsible Officer may recommend revisions to the Policy consistent with approval authorities and applicable Bylaws, Standing Orders, and Polices of the Regents.

C. ***Approval of Actions***

Actions prescribed in this Policy must be approved and implemented in accordance with the local procedures.

D. ***Compliance with the Policy***

The Executive Officer at each Location will designate a local management office that is responsible for monitoring and reporting compliance with this Policy. The Senior Vice President-Chief Compliance and Audit Officer must periodically audit and monitor compliance with this Policy.

E. ***Noncompliance with the Policy***

Noncompliance with this Policy is handled in accordance with academic and staff personnel and student policies pertaining to disciplinary matters.

V. PROCEDURES

1. Each Executive Officer, or designee(s), must establish and implement local procedures consistent with this Policy including, but not limited to:

2. Designating a point of contact office responsible for VS/SS content integrity and the prevention of misuse of Video Data.

3. Defining processes for approving installation of new VS/SS equipment, maintaining operational equipment, and decommissioning old VS/SS equipment and Video Data.

4. Defining an exception protocol for use of personally owned cameras for VS/SS activity.

5. Instituting security protocols, including regularly scheduled equipment checks, for the prevention of tampering with VS/SS equipment and Video Data.

6. Implementing procedures for requesting and approving access to Video Data.

7. Developing processes for notification that VS/SS is recording an area.

8. Designating, and providing notification of, local Private Spaces and Sensitive Areas.

9. Ensuring completion of VS/SS technical training by video operators and for any individual reviewing Video Data. Each location will implement procedures to record and track training compliance.

10. Designating a local office responsible for monitoring and reporting compliance with this Policy.

11. Designating a local point of contact to answer questions regarding video security and safety.

Any exception to local procedures required by the Policy must be reviewed and approved by the Executive Officer or designee(s).

VI. RELATED INFORMATION

A. UC Statement of Privacy Values and Privacy Principles
B. Electronic Information Security; UC Business and Finance Bulletin IS-3
C. Appendix - Data Security and Privacy
D. UC Standards of Ethical Conduct
E. UC Standards of Ethical Values
F. Sexual Violence and Sexual Harassment Policy, University of California
G. Nondiscrimination Policy Statement for University of California Publications Regarding Student-Related Matters.
H. University of California Non-Discrimination Policy
I. Student-Related Policy Applying to Nondiscrimination on the Basis of Sex
J. Electronic Communications Policy, University of California, 2005
K. PACAOS-102.25
L. Policy for Cash and Cash Equivalents Received, BUS 49, Section IX (14) Physical Security
M. BFB-RMP-2: Records Retention and. Disposition: Principles, Processes, and Guidelines.
N. 45 CFR Part 160&Part 164, subparts A&C Security Standards: Physical Safeguards (Protected Health Information)
O. Placeholder for: UC Police Gold Book, Body Camera section
P. California Public Records Act
Q. California Information Practices Act of 1977

VII. FREQUENTLY ASKED QUESTIONS

1. ***What are best practices in the use of VS/SS?***
Suggested best practices include, but are not limited to:

- Use of technical standards that meet a minimum video quality measure
- Use of a visible date and timestamp on all recorded images
- Automatic uploading from VS/SS equipment to a Video Data storage location which facilitates regular review and over-write capabilities.

- Consistent procedures for the use of VS/SS equipment and review of the associated Video Data.

- Technical compatibility with the devices and/or Video Data which are regularly obtained and used by campus police including but not limited to body-worn and vehicle-mounted cameras.

- When feasible each VS/SS installed and used at a UC Location should be integrated with the campus police department security systems or in the case of healthcare systems, integrated in a Security Monitoring Center.

- All equipment associated with a VS/SS must be operational at all times. When not working, this equipment must be removed, including associated signage.

- Use of privacy impact assessments and information security risk assessments prior to the installation of new VS/SS.

VIII. REVISION HISTORY

This is the initial issuance of this Policy.