

Systemwide Video Security Camera Policy April 29, 2020

I. PURPOSE

The purpose of this document is to provide a systemwide policy for the installation and use of Video Security Cameras. All recording shall be done with recognition of the reasonable expectation of privacy among members of the University community. This policy shall supersede all campus policies that cover matters within the scope of this policy. This Policy does not apply to members of the University Police Department acting in the normal course and scope of their assigned duties.

II. ORGANIZATIONS AFFECTED:

This policy applies to all organizational units of the University and all University property. University auxiliaries are required to comply with this policy.

III. DEFINITIONS:

- a. *Monitoring*: Refers to the live viewing of recorded images from cameras and monitors that have been approved for use on the campus for the purpose of enhancing security, safety, and aiding law enforcement.
- b. *Video Security Cameras*: A camera device that is capable of capturing images viewable by the naked eye and transferring such images to a data storage system which may be established by the University as a part of the campus infrastructure. Cameras installed pursuant to this policy shall not be used to capture audio.
- c. *Area in which there is a reasonable expectation of privacy*: An area such as a private office (including shared offices), cubicles that are normally not accessible to the general public, employee break rooms, bathroom, shower room, locker room, lactation room, changing room, or area where a reasonable person might change clothes.
- d. *Public Area*: An area open to public use, where no reasonable expectation of privacy exists. Public areas include, but are not limited to, parking lots and structures, hallways, library study rooms, buildings open to the general public, and all outdoor areas.
- e. *University Property*: All property owned, leased, and/or operated by CSU and its campuses, except any interior property which is solely managed and operated by a third party.
- f. *University Police Department*: The term "University Police Department" as used in this Policy refers to the department on each campus that performs the police function,

Systemwide Video Security Camera Policy
April 29, 2020

whether the Department of Public Safety, Police Department or Police Services, regardless of the title.

- g. *Chief of Police*: The term "Chief of Police" as used in this Policy refers to the individual on each campus who manages the Department of Public Safety, Police Department or Police Services, regardless of whether the individual possesses the title Chief of Police, Director of Public Safety or some other title as determined by the President or Chancellor.

IV. Use of Data

- a. Video Security Camera footage may be monitored and reviewed by University Police in accordance with this policy, and as authorized by the Chief of Police.
- b. Video Security Camera data must be consistent with the provisions of this Policy. Video Security Cameras shall not be used for the supervision of employees. This includes but is not limited to, use for time-keeping and attendance, examination of work, and evaluations. For purposes of this policy only, the CSU shall not install cameras in the inside of custodial closets.
- c. CSU will not continuously monitor video footage for employee conduct. Further, video security cameras shall not view or monitor employee computer screens or workstations. Further, absent an allegation or complaint, CSU will not review video security footage for the purposes of identifying employee misconduct. Video footage may be used to corroborate, prove or disprove specific acts of misconduct. Video footage shall not be used to prove or disprove allegations related to attendance or timekeeping. Notwithstanding the above, CSU may review video security footage in the event University Police determines the footage depicts an incident for which the police have a legal obligation to report or when monitoring is legally required.

It is explicitly understood that a request to review video based on an approximate date and time of an alleged incident might reveal misconduct separate from the alleged incident and that such specific misconduct found incidental to a request made within the parameters of this policy may be used to corroborate, prove or disprove specific acts of misconduct consistent with this section.

Nothing in this section limits CSU's right to use video footage in connection with student discipline.

If a request is made to the University Police Department and approved by the President, or President's designee, the footage will be encrypted, copied and provided to the employee or student who has been served with a Notice of Discipline.

Systemwide Video Security Camera Policy
April 29, 2020

- d. The Chief of Police may only review Video Security Camera data relating to supervision of Police Officers employed within the University Police Department where:
- i. The Chief of Police is aware of a specific incident, and/or has received a complaint in respect of individual(s) conduct; and
 - ii. The University has a duty to further investigate the circumstances of the incident and/or complaint pursuant to CSU policy and/or state/federal law; and
 - iii. The review is to be undertaken in the normal course and scope of the Chief's duties.

V. PROCEDURE

a. Use of Video Security Cameras

The University may employ Video Security Cameras in public areas on University Property for any legitimate purpose including, but not limited to, deterring crime, assisting police in criminal investigations, and protecting the safety and property of the campus community. Video Security cameras may be used in areas where academic instruction takes place where there are serious security concerns. Any use of Video Security Cameras must conform to state and federal law.

The following uses of Video Security Cameras on campus do not require approval:

1. Video Security Cameras used specifically to monitor testing locations, lab environments.
2. Covert University Police Department or other law enforcement agency operations for criminal surveillance as governed by federal or state law.
3. Video Security Cameras used specifically to safeguard money, valuable or confidential documents, pharmaceuticals or high value equipment or supplies from theft, destruction, or tampering.

b. Installation and Management of Video Security Cameras

Installation and use of Video Security Cameras on campus requires the approval of the University Police Department.

Systemwide Video Security Camera Policy
April 29, 2020

Video Security Camera placement shall be in public areas and viewing angles shall be appropriate for security and law enforcement purposes. Except as otherwise provided herein, Video Security Cameras may not be established to view or monitor employees computer screens or workstations or other areas where there is a reasonable expectation of privacy, nor will they be directed or zoomed into the windows of any private residential building including residence halls.

The University Police Department will:

1. Monitor requests for the installation and/or enhancement of Video Security Camera systems, and maintain a record of the location and type of Video Security Cameras approved for installation.
2. Approve or deny any requests for installation of Video Security Camera systems.
3. Document requests to view footage in a master log maintained for that purpose. This log shall include requestor's name, date of request, the reason for the request, approximate date and time of incident, approver's name, and date of approval.
4. Document abuse and misuse of Video Security Camera monitoring systems and equipment.
5. Oversee installation of Video Security Camera systems or manage any vendor who installs the systems.
6. Ensure compliance of Video Security Cameras systems with applicable regulation.
7. Control and limit access to Video Security Camera data storage systems.
8. Create procedures for storage, disposal, and retrieval of Video Security Camera content.
9. Provide training on appropriate use of Video Security cameras.

The University Police Department may seek assistance from Information Technology Services.

c. Notice

Posting of Notice that Video Security Cameras are present is required at least at all campus entrances and at the entrance to any specific public area monitored by a Video Security Camera at which there may otherwise be a reasonable expectation of privacy (such as a room known to be used by employees to change clothes). Notices should include a campus contact number; e.g. "NOTICE: This area is subject to security video camera recording. For information, please contact the California State University, [Campus] Police Department at [phone number].

Systemwide Video Security Camera Policy
April 29, 2020

d. Review of Data

- i. Pursuant to Section IV of this policy Video Security Camera footage may only be monitored and reviewed by University Police Department personnel, and as authorized by the Chief of Police. Student employees shall not be used to monitor or review Video Security Camera footage.
- ii. The Chief of Police or designated law enforcement administrator may approve a written request to review Video Security Camera data by the President; Vice Presidents; administrators responsible for overseeing police; Directors or Associate Vice Presidents of human resources, Directors or Associate Vice Presidents of faculty personnel, and Directors or Associate Vice Presidents of Title IX and/or equal opportunity offices, provided that the Chief is satisfied that the request is for a purpose authorized by this policy and that the requirements of Section IV(c) and/or (d) are met.

Vice Presidents; administrators responsible for overseeing police; Directors or Associate Vice Presidents of human resources, Directors or Associate Vice Presidents of faculty personnel, and Directors or Associate Vice Presidents of Title IX and/or equal opportunity offices making the request shall not be the direct supervisor of the employee whose alleged misconduct is suspected of being captured on the Video Security data.

- iii. The University will release Video Security Camera data when required under the Public Records Act, the Higher Education Employer-Employee Relations Act, a Collective Bargaining Agreement, or as otherwise required by law. This provision is not intended to abridge established employee due process rights.
- iv. The Union shall only be given the general location of security cameras, unless otherwise required by the Public Records Act, Higher Education Employer-Employee Relations Act, a Collective Bargaining Agreement, or otherwise required by law. Access to specific location or specific information regarding cameras and their locations shall be limited to: campus police; the President; Vice Presidents; administrators responsible for overseeing police; Directors or Associate Vice Presidents of human resources, Directors or Associate Vice Presidents of faculty personnel, and Directors or Associate Vice Presidents of Title IX and/or equal opportunity offices.
- v. If the Union believes that a particular camera is capturing an area where a reasonable expectation of privacy exists, the Union may request that a statewide Union representative view on a monitor the field of vision from that specific camera. This shall be viewable at the Campus police station, by the Chief of Police or their designee. If after viewing the Union continues to

Systemwide Video Security Camera Policy
April 29, 2020

believe that the camera violates an employee's reasonable expectation of privacy, the Union may file a written request to change the location or limit the visual range of a specific installation of video monitoring equipment based on a belief that it infringes on individual privacy or other protected rights. The request shall be submitted to the Vice President for Administration, and shall (a) identify the location, (b) identify the right believed to be infringed, (c) provide an explanation of how the video device installation infringes that right. The Vice President of Administration will respond to the request within fourteen (14) business days after receipt. The response will be based on a thorough reconsideration of the initial request to install the devices in light of the concerns.

In the interest of public safety, the Union agrees that the labor representative having access to the footage shall not disclose details about camera locations, field of view, or any other details learned about the video security cameras subject to this policy except to those persons directly impacted by the camera footage.

For FERPA purposes, Video Security Camera recordings with information about a specific student are considered law enforcement records unless the University uses the recording for student disciplinary purposes or makes the recording part of the educational record.

e. Data Storage

Video Security Camera images should be stored in encrypted formats both in storage and in transit where feasible. Where not feasible, adequate safeguards should be documented regarding physical and logical access as well as integrity and non-repudiation.

Video Security Camera recorded images should be retained for a minimum of thirty (30) days. Recordings should be erased or recorded over in a secure manner after thirty (30) days in the absence of a compelling reason to retain or a request from the Chief of Police, Office of General Counsel or the Vice President of Business/CFO, or their designee. Units should follow the procedures provided by Property Disposition <Insert Link> to sanitize, wipe, or destroy.

In the following instances Video Security Camera recorded images must be retained for at least five (5) years after the subject employee's separation from the CSU, or five years after the incident, accident, or other circumstance has been finally resolved, whichever occurs later. Campus counsel shall review all such requests for data to be retained for at least five (5) years.

**Systemwide Video Security Camera Policy
April 29, 2020**

1. The Video Security Camera image records a known incident or accident;
2. Demonstrated business need approved by the VP/CFO or delegated authority; and/or
3. Grantor or funding agency requirement. The VP/CFO or delegated authority must approve in advance and in writing the preservation and storage by any unit of all other security camera data for greater than thirty (30) days.


Retention required for a litigation hold, requested for an ongoing proceeding underway (including but not limited to, an ongoing criminal or civil court proceeding, employment investigation, or legal hold or court order), and does not require further review by Campus Counsel.

f. Contact

Questions regarding this policy should be directed to Assistant Vice Chancellor, Business and Finance Operations Support, California State University Office of the Chancellor.

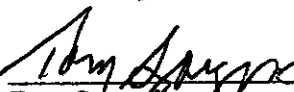
The Assistance Vice Chancellor, Business and Finance Operations Support is Mr. Michael Redmond. Email: Mredmond@calstate.edu; phone number: (562) 951-4345

CSUEU



 Rocky Sanchez
 Vice President for Representation
 DocuSigned by:
 Rocky Sanchez
 E8429B0D0E1547B

Tessy Reese
 BU 2 Chairperson
 DocuSigned by:
 Tessy Reese
 85AF00AE804044A
 Fortunato Garcia
 BU 5 Chairperson



 Tony Spraggins
 BU 6 Chairperson
 DocuSigned by:
 Rich McGee
 50C2A892200C419

Rich McGee
 BU 9 Chairperson
 DocuSigned by:
 Brian Young
 788037C1C68F465
 Brian Young
 Chief Negotiator

DocuSigned by:


 Pam Robertson
 BU 2 Vice Chairperson
 DocuSigned by:
 Don Moreno
 DCC2D8571F36433

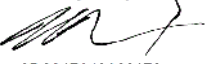
Don Moreno
 BU 5 Vice Chairperson
 DocuSigned by:
 Annabelle Siongco
 181E910C89C044F

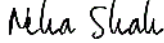
Annabelle Siongco
 BU 7 Vice Chairperson
 DocuSigned by:
 Martin Brenner
 4006F35022884F3

Martin Brenner
 BU 9 Vice Chairperson
 DocuSigned by:
 Andrew Heller
 Andrew Heller 27
 Labor Relations Representative

Systemwide Video Security Camera Policy
April 29, 2020

CSU

DocuSigned by:

9DC84FA12A664F8...
Assistant Vice Chancellor

DocuSigned by:

7C7CA824988C44F...
Chief Negotiator