Subject:	Department Name:	Effective Date:
Video Surveillance & Access Control Policy, Procedures and Guidelines	Business & Finance	Issue Date: 11/10/15
	Policy	Approval:

1. **Purpose**

The CSU Stanislaus Police Department (UPD) is charged with reviewing, recommending, approving, and managing proposed and existing video surveillance and access control security equipment and software applications. To ensure the ability to use the data, the systems need to be standardized and made easily accessible to the UPD. UPD will seek assistance in conducting its review from the Office of Information Technology (OIT) and Facilities Services.

Video and access control security applications serve three primary purposes:

a. If an area is posted as being under video recording or surveillance, video security applications can be a crime deterrent.
b. Once a crime has been committed, the video security and access control applications can assist in the identification of the responsible parties.
c. Access control systems can improve physical security by reducing the risk of unauthorized access, and in certain circumstances can help meet physical security audit objectives.

This policy addresses video applications not covered by existing rules or by policies related to academic research. Any video application related to research must also be approved pursuant to applicable research policies, such as those administered by the Institutional Review Board.

2. **Definitions**

Access Control: The use of computer-controlled entry and locking devices to limit and log access to areas of a physical facility, usually by means of a digitally-enclosed identification card or biometric device.

Institutional Review Board: The mission of the Institutional Review Board at CSU Stanislaus is to promote the ethical conduct of student, staff, and faculty research involving human subjects through safeguarding the rights and welfare of the research subjects therein. http://www.csustan.edu/UIRB/

Video Surveillance: The use of image capture, processing, transmission and storage equipment for authorized monitoring of public areas. This includes full-motion and still images, use of network transmission capacity, and digital storage and retrieval software. Audio recording is specifically **excluded** from this definition.

Workstation: For the purposes of this policy, a workstation includes private offices, desks or cubicles and will not be monitored.

3. **Scope of Policy**

This policy applies to all CSU Stanislaus Departments, Colleges, Divisions, and Auxiliaries (hereafter known as "University". This policy does not address the use of general-purpose web cameras for special interest applications or University promotion purposes, but it should be noted that such cameras must not be used as a substitute for a security system.

4. **Policy**

The CSU Stanislaus Police Department (UPD) must review and approve any proposed or existing installation of video or access control security applications on properties owned, leased, or controlled by the University. All video and access control security applications must conform to federal and state law in addition to University policy. Video and access control security applications must conform to standards established by the UPD so recorded data and log records are easily retrievable.

Video monitoring will not be used to view or record workstations, including private offices, desks or cubicles, except the work counter where cashiering services are performed or money is exchanged during the regular course of business; classrooms, or rooms where students, staff and/or faculty commonly work, study or hold discussions; living areas, or other common-use areas where a reasonable expectation of privacy exists. Cashier area shall be monitored, but no cameras shall be placed such that cashiers are monitored.

Video and access control security records will not be used for purposes related to the evaluation of employee job performance, nor will they be used as a means to track employee attendance and/or as a timekeeping record. However, the University may use such records in support of disciplinary proceedings against faculty, staff, or student(s), in a civil suit against person(s) whose activities are shown on the recording and are the basis for the suit. Review of video records shall only be performed by an authorized Police Department administrator, Police Officer or dispatcher, with a good faith reason for the review.

Nothing in this policy shall be interpreted to prevent the use of video monitoring or surveillance in connection with an active criminal investigation or specific court order.

Cameras will not be monitored in real time with the exception of those located in the University Police Department; as an immediate response to the report of criminal activity on campus; suspicious behavior or in the course of an ongoing investigation of criminal activity. Cameras shall only be reviewed and monitored by an authorized person including a student, dispatcher or Police Department administrator with a good faith reason for the review.

Any person who tampers with or destroys a camera or any part of the electronic surveillance system may be prosecuted in the criminal justice system as well as the campus judicial system.

This policy will be updated as necessary to reflect changes in the University's academic, administrative, or technical environments, or applicable federal/state laws and regulations.

5. Responsibilities

5.1 University Police (UPD) Responsibilities:

a. UPD is responsible for overseeing an annual review of this policy and communicating any changes or additions to appropriate CSU Stanislaus personnel.
b. UPD reviews, approves, and oversees the installation, servicing, and management of video and access control security applications.
c. UPD monitors developments in relevant laws and in the security industry to assure that video monitoring and access control on University property is consistent with the highest standards and protections.
d. UPD maintains a database of all University-owned or -controlled camera and door access control locations.
e. UPD receives all requests for the release of recordings and logs obtained through video security and access control applications.
f. UPD releases video security and access control applications data upon authorization by the Chief of Police or designee. No other University department may release data obtained through video security and access control applications.
g. UPD documents the release of any video security and access control applications data.
h. UPD will notify The Office of Faculty Affairs and Human Resources (FA/HR) of any proposed changes to this policy and FA/HR will provide a 30-day notice of the proposed changes to the Unions.
i. UPD will notify FA/HR of the plans to install new cameras and FA/HR will provide 30-day notice of the proposed installation to the Unions.
j. FA/HR will certify in writing to the unions that cameras are in compliance with this policy prior to cameras being activated.

5.2 Campus Departments Responsibilities

a. Departments with existing video security or access control applications must have their applications reviewed by the UPD and brought into conformance with campus standards.
b. Departments wishing to install new video security and access control applications must submit their request to UPD, OIT and Facilities for review. The request shall be in writing stating the reason, the number and location for a camera installation.
c. Department heads or their designees charged with overseeing video security and access control applications must arrange for UPD management of their video security and access control applications.

5.3 Office of Information Technology & Facilities Services Responsibilities:

a. OIT reviews and consults with the University Police Department regarding the selection and installation of video security and access control systems and equipment.
b. OIT defines technical standards for the equipment and software applications, provides network and central server/storage support for the system, and provides software support, troubleshooting and configuration assistance. OIT staff is not permitted to access system controls or electronic records except as required in order to fulfill installation and maintenance responsibilities.
c. Facilities Services coordinates the installation and maintenance of equipment and ensures compliance with all relevant building and fire codes.

6. Governing Law

The installation or use of any device for photographing, observing, or eavesdropping actions or audio in a "private" place without permission of those being observed or listened to is a crime punishable by law. A private place is defined as a location where a person expects to be safe from unauthorized surveillance.

In contrast, silent video surveillance (involving no recording of sounds) in public places is permissible. Individuals and transactions in plain view in a public setting have no reasonable expectation of privacy; therefore the use of video is allowable. See United States vs. Sherman, 990 F. 2nd 1265 (9th Cir. 1993); Dow Chemical Co. vs. United States, 106 **S. Ct. 1819 (1986); People vs. Mackey, 121 Michigan App. 748, 329 N.W. 2nd 476 (1982).**

7. Procedures and Guidelines

a. Video and access control review or monitoring for security purposes will be conducted in a professional, ethical, and legal manner. Personnel involved in video review or monitoring will be appropriately trained and supervised in the responsible use of this technology.

b. The UPD will not approve camera positions with views of residential spaces, with the exception of the use of video monitoring for criminal investigations. The focus of cameras used in video surveillance will not cover areas where there is an expectation of privacy. This does not preclude monitoring the exterior of buildings, building lobbies, parking lots, roadways, or exterior public areas and venues such as the stadium or Amphitheater.

c. Monitoring will be conducted in a manner consistent with all existing University policies, including non-discrimination, sexual harassment, and other relevant policies. Camera control operators will not monitor individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other protected classifications.

d. Camera control operators and / or managers of video security applications will not seek out or continuously view people being intimate in public areas.

e. Camera control operators and / or managers of video security applications will not view workstations including private offices, desks or cubicles, except the work counter where cashiering services are performed or money is exchanged during the regular course of business; classrooms, or rooms where students, staff and/or faculty commonly work, study or hold discussions; living areas, or other common use areas where there is a reasonable expectation of privacy.

f. Camera control operators will be trained in the technical, legal, and ethical parameters of appropriate camera use. Camera control operators and / or managers of video surveillance applications will receive a copy of the *Video Surveillance & Access Control Policy* and will provide written acknowledgement that

they have read and understood it. Failure to provide written acknowledgement does not excuse violation of the policy.

g. Information obtained in violation of the *Video Surveillance & Access Control Policy* may not be used in a disciplinary proceeding against a member of the University's faculty, staff, or student population. It is not the intent of this policy to use video cameras for the monitoring of employees for disciplinary purposes, performance evaluation, or corrective action.

h. The following signage shall be required by the UPD at public locations monitored by video surveillance: "THIS AREA IS SUBJECT TO VIDEO RECORDING: For more information, contact UPD at 667-3114". An exception to this recommendation would be if announcing the use of video surveillance would undermine its purpose such as in the investigation of criminal activity.

i. Dummy cameras are prohibited, as they could lead the viewer to a false sense of security that someone is monitoring the cameras.

j. Campus units approved by UPD to install video surveillance systems will permit access to their application via the campus network for maintenance, auditing, and police investigations.

k. Each campus unit with video and access control security applications must provide the UPD with a list of people who can be contacted about the application during business hours and after hours.

l. Installation of video and access control security applications are the financial responsibility of the requesting unit. This responsibility includes the cost of required hardware and software, network and device installation, facilities charges, service and maintenance.

m. Any person who tampers with or destroys a camera or any part of the electronic surveillance system may be prosecuted in the criminal justice system as well as the campus judicial system.

n. To maintain an informed University community, UPD will periodically disseminate written materials describing the purpose of video monitoring and the guidelines for its use. The location of permanent video cameras will be published in the Annual Campus Security Report.

o. All storage and access to recordings will be controlled by UPD:

i. Recordings used in law enforcement investigations or criminal prosecutions shall be retained until the end of the court or judicial proceedings and appeal period unless directed otherwise by a court.

ii. Recordings may also be retained for other bona fide reasons as determined by UPD, in consultation with General Counsel.

iii. Recordings shall be retained for 45 days and then will be immediately erased or recorded over, or otherwise destroyed, unless retained as part of a disciplinary matter, a criminal investigation, a civil or criminal court proceeding, pursuant to a Preservation Notice issued by the Office of the General Counsel. No attempt shall ever be made to alter any recording. Editing or otherwise altering recordings or still images, except to enhance quality for investigative purposes or blur features as described above, is strictly prohibited.

iv. Recordings retained as part of a disciplinary matter, a criminal investigation, or a civil or criminal court proceeding, will be destroyed at the appropriate time, which will be determined and directed by General Counsel, and in consultation with The Office of Faculty Affairs and Human Resources when appropriate.

v. Transmission of recordings using the Internet or campus network will use encryption technology to ensure that recordings are not improperly accessed.

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

vii. Only the UPD may release data produced by video and access control security applications. Any release will be conducted in accordance with applicable laws and consistent with the *Video Surveillance & Access Control Policy.*

p. Violations of the procedures for video and access control review or monitoring referenced in the *Video Surveillance & Access Control Policy* will result in disciplinary action consistent with the rules and regulations governing University employees.