Section:	Safety Operations
Policy Name:	Surveillance Cameras
Policy Number:	
Policy Owner:	Safety Operations Director
Responsible University Office:	University Safety Operations
Origination Date:	
Effective Date:	
Revisions:	
Review Schedule:	As needed
Last Reviewed:	
Authority:	

I. Scope of Policy

The University of La Verne is committed to enhancing the quality of life of the campus community by integrating the best practices of safety and security with technology. A critical component of a comprehensive security plan is the utilization of a security and safety camera system. The surveillance of public areas is intended to deter crime and assist in protecting the safety and property of the University of La Verne community. This policy addresses the university's safety and security needs while respecting and preserving individual privacy.

To ensure the protection of individual privacy rights in accordance with the university's core values and state and federal laws, this policy is adopted to formalize procedures for the installation of surveillance equipment and the handling, viewing, retention, dissemination, and destruction of surveillance records. The purpose of this policy is to regulate the use of camera systems used to observe and record public areas for the purposes of safety and security. The existence of this policy does not imply or guarantee that cameras will be monitored in real time 24 hours a day, seven days a week.

II. Policy Statement

The University of La Verne Campus Safety Department (ULVCSD) has the authority to select, coordinate, operate, manage, and monitor all campus security surveillance systems pursuant to this policy. All departments using camera surveillance are responsible for implementing and complying with this policy in their respective operations. All existing uses of security camera systems will be required to comply with the policy at a future date. A notification of the compliance date will be made 12 months in advance. Unapproved or nonconforming devices will be removed prior to the compliance date.

This policy applies to all personnel, departments, and colleges of the University of La Verne in the use of security cameras and their video monitoring and recording systems. Security cameras may be installed in situations and places where the security and safety of either property or persons would be enhanced. Cameras will be limited to uses that do not violate the reasonable expectation of privacy as defined by law. Where appropriate, the cameras may be placed campus-wide, inside and outside buildings. Although the physical cameras may be identical, the functions of these cameras fall into three main categories:

III. Policy Standards and Procedures

A. Responsibilities

1. Facilities, Information Technology and the ULVCSD are responsible for advising departments on appropriate applications of surveillance technologies and for providing technical assistance to departments preparing proposals for the purchase and installation of security camera systems.
2. ULVSCD and Information Technology shall monitor developments in the law and in security industry practices and technology to ensure that camera surveillance is consistent with the best practices and complies with all federal and state laws.
3. ULVSCD, Facilities and Information Technology will review proposals and recommendations for camera installations and review specific camera locations to determine that the perimeter of view of fixed location cameras conforms to this policy. Proposals for the installation of surveillance cameras shall be reviewed by the Director of Campus Safety or designee.
4. ULVSCD will assess new camera locations. An annual evaluation of existing camera locations and incidents will be conducted.
5. ULVSCD will review any complaints regarding the utilization of surveillance camera systems and determine whether this policy is being followed. Appeals of a decision made by the Director of Safety Operations will be made to and reviewed by the SOC which will make a recommendation to the Vice President for Facilities, and Information Technology Services, who will render a decision.

B. Property Protection:

Where the main intent is to capture video and store it on a remote device so that if property is reported stolen or damaged, the video may show the perpetrator. Examples: an unstaffed computer lab, unstaffed science lab, or a parking lot.

C. Personal Safety:

Where the main intent is to capture video and store it on a remote device so that if a person is assaulted, the video may show the perpetrator. Examples: a public walkway, or a parking lot.

D. Extended Responsibility:

Where the main intent is to have the live video stream in one area monitored by a staff member in close proximity. In this case video may or may not be recorded. Example: a computer lab with multiple rooms and only one staff.

E. General Principles

1. Information obtained from the cameras shall be used for safety and security purposes and for law and policy enforcement, including, where appropriate, student judicial functions. Information must be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure.
2. All appropriate measures must be taken to protect an individual's right to privacy and hold university information securely through its creation, storage, transmission, use, and deletion.
3. All camera installations are subject to federal and state laws.

4. Departments requesting security cameras will be required to follow the procedures outlined in this policy.

IV. Placement of Cameras and Monitoring

A. The locations where cameras are installed may be restricted access sites such as a departmental computer lab; however, these locations are not places where a person has a reasonable expectation of privacy. Cameras will be located so that personal privacy is maximized. No audio shall be recorded except in areas where no one is routinely permitted. Requests to utilize audio surveillance that does not comply with this requirement will be evaluated on a case by case basis by the SOC.

Camera positions and views of residential housing shall be limited. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy.

Unless the camera is being used for criminal investigations, monitoring by security cameras in the following locations is prohibited:

- Student dormitory rooms in the residence halls
- Bathrooms
- Locker rooms
- Offices
- Classrooms not used as a lab

Unless being used for criminal investigations, all video camera installations should be visible.

B. Access and Monitoring

1. All recording or monitoring of activities of individuals or groups by university security cameras will be conducted in a manner consistent with university policies, state and federal laws, and will not be based on the subjects' personal characteristics, including age, color, disability, gender, national origin, race, religion, sexual orientation, or other protected characteristics. Furthermore, all recording or monitoring will be conducted in a professional, ethical, and legal manner. All personnel with access to university security cameras should be trained in the effective, legal, and ethical use of monitoring equipment.
2. University security cameras are not monitored continuously under normal operating conditions but may be monitored for legitimate safety and security purposes that include, but are not limited to, the following: high risk areas, restricted access areas/locations, in response to an alarm, special events, and specific investigations authorized by the Director of Safety Operations or designee.
3. For Property Protection and Personal Safety cameras, access to live video or recorded video from cameras shall be limited to authorized personnel of the department which installed the cameras, the Campus Safety Department and other persons authorized by the Director of Safety Operations or designee. The copying, duplicating and/or retransmission of live or recorded video shall be limited to persons authorized by the Director of Safety Operations or designee.
4. A record log will be kept of all instances of access to, and use of, recorded material. Nothing in this section is intended to limit the authority of the law enforcement activities.

C. Appropriate Use and Confidentiality

1. Personnel are prohibited from using or disseminating information acquired from university security cameras, except for official purposes. All information and/or observations made in the use of security cameras are considered confidential and can only be used for official university and law enforcement purposes.

D. Use of Cameras for Criminal Investigations

1. The use of mobile or hidden video equipment may be used in criminal investigations by the Law Enforcement after proper notification to the Universities Director of Safety Operations. Covert video equipment may also be used for non-criminal investigations of specific instances which may be a significant risk to public safety, security and property as authorized by the Senior Director of Safety Operations or designee.

E. Exceptions

1. This policy does not apply to cameras used for academic purposes. Cameras that are used for research would be governed by other policies involving human subjects and are, therefore, excluded from this policy.
2. This policy does not address the use of Webcams for general use by the university. This policy also does not apply to the use of video equipment for the recording of public performances or events, interviews, or other use for broadcast or educational purposes. Examples of such excluded activities would include videotaping of athletic events for post-game review, videotaping of concerts, plays, and lectures, or videotaped interviews of persons. Automated teller machines (ATMs), which may utilize cameras, are exempt from this policy.

F. Installation

1. Individual colleges, departments, programs, or campus organizations installing video surveillance equipment shall submit a written request to their appropriate dean or vice president describing the proposed location of surveillance devices, justifying the proposed installation, and identifying the funding source or sources for purchase and ongoing maintenance.
    a. The vice president, dean or designee will review the request and recommend it to the Director of Safety Operations, if appropriate.
    b. The Director of Safety Operations or designee will review all proposals from deans and vice presidents. Upon completion of review of the project, the Director of Safety Operations will forward the proposal to the SOC with a recommendation.
    c. The SOC will be responsible for reviewing and approving or denying all proposals for security camera equipment recommended by the Director of Safety Operations. The SOC will take into consideration urgency, placement of the system and existing infrastructure where the camera will be installed, bandwidth needed and storage availability.
2. Purchasing will not accept, approve, or process any order for security camera systems without the approval of the SOC.

G. Operation

1. Video surveillance will be conducted in a manner consistent with all existing university policies.
2. Campus Safety Officers shall monitor based on suspicious behavior, not individual characteristics.
3. Campus Safety Officers shall not view private rooms or areas through windows.
4. All Campus Safety Officers and Supervisors involved in video surveillance will perform their duties in accordance with this policy.

H. Storage and Retention of Recordings

1. No attempt shall be made to alter any part of any surveillance recording. Surveillance centers and monitors will be configured to prevent camera operators from tampering with or duplicating recorded information.
2. Surveillance records shall not be stored by individual departments. All surveillance records shall be stored in a secure university centralized location for a period of 30 days and will then promptly be erased or written over, unless retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Director of Safety Operations or designee. Individual departments shall not store video surveillance recordings.
3. A log shall be maintained of all instances of access to or use of surveillance records. The log shall include the date and identification of the person or persons to whom access was granted.
4. Surveillance records shall be maintained to preserve incidents that may potentially be part of litigation.