STANFORD UNIVERSITY

Stanford University
Video Surveillance System Guidelines

Effective Date: May 1, 2014

Video Surveillance System Guidelines Statement

All Stanford University ("Stanford")[1] implemented and controlled video surveillance, monitoring, and recording applications and installations (Video Surveillance Systems) must conform to the Stanford Video Surveillance System Guidelines unless an exception is requested and approved by the Video Surveillance Governance Group ("VSGG"). The VSGG consists of representatives from Stanford University's Department of Public Safety (SUDPS), Office of Risk Management (ORM), and the Office of General Counsel (OGC). Except as provided in these Guidelines, Video Surveillance Systems will not be used to view, monitor, or record private spaces. However, nothing in these Guidelines prevent the use of Video Surveillance Systems in connection with an active criminal investigation or specific court order. Stanford reserves the right to review and approve any proposed or existing Video Surveillance Systems on properties owned, leased, managed, or controlled by Stanford.

Design Principles and Practices

Video Surveillance Systems are a component of a comprehensive and integrated approach to security, which includes

- Access control, including card access and key control.
- Issuance of identity credentials and authorization.
- Security systems.
- Crime Prevention Through Environmental Design (CPTED) which includes strategies such as lighting, landscaping, and building and site circulation patterns in the security design.
- Security policies, procedures, and practices, including SUDPS and private security officer resources.
- To ensure the forensic value of the data, the Video Surveillance Systems need to be compatible with the Stanford enterprise system and accessible to SUDPS upon lawful request.

The intent of these Guidelines is to establish approved written documentation for the design, use, operation and maintenance of Video Surveillance Systems. Additionally, it is the intent of these Guidelines to be conceptual and risk-based. However, there may be alternate methods employed to obtain the desired results of the applicant.

Prior to installation, a Security Vulnerability Assessment ("Assessment") should be performed by SUDPS for each Video Surveillance System project. The Assessment consists of a review of the physical security and security policies and procedures. The findings and recommendations included in the Assessment may be evaluated by the VSGG and should be incorporated in the system design.

[1] For the purposes of these Guidelines Stanford excludes actions that SUDPS may take to investigate criminal activity. These Guidelines only cover the use of video technology for the purposes of surveillance for safety and security. Other uses of video technology at Stanford are beyond the scope of these Guidelines.

Who Administers These Guidelines

The VSGG administers these Guidelines. SUDPS is charged with reviewing, recommending, approving, and managing proposed and existing Video Surveillance System applications. SUDPS is available to discuss and review security programs and operations with Stanford building managers, zone managers, project managers, and with managers of tenant-operated facilities and programs.

Who Is Affected by These Guidelines

- Any Stanford department that uses a Video Surveillance System for the purpose of safety or security in any location owned, leased, managed, or controlled by Stanford.
- Planners, architects, and designers for all construction projects at Stanford.
- Internal Stanford users and lease tenants on Stanford property.
- Stanford as a tenant. (Stanford should negotiate these requirements with landlords, where possible.)

Value and Expectations

Security systems, including Video Surveillance Systems, are intended to assist in mitigating risk to people, property (including buildings and building assets), and the educational and operational processes at Stanford. The systems can provide the following security and safety features:

- Video Surveillance Systems may serve as a crime deterrent.
- Once a crime has been committed, the systems may assist in the identification of the responsible parties.
- Video surveillance of approved locations can provide a date and time stamped video record of the presence of specific people at specific locations, including those who have entered or exited a location.
- The focus of Video Surveillance Systems at Stanford is to record activity of building entrance and exit points and perimeter doors. This does not preclude monitoring of the exterior of buildings or building lobbies. Where additional security measures are recommended based on the Security Vulnerability Assessment, cameras should be installed to view other areas identified in the Assessment as appropriate.
- Video surveillance of areas deemed by SUDPS or VSGG to be high-risk, including certain types of laboratories; mission critical buildings such as data centers and energy facilities; large venues such as stadium, arena, theaters; hazardous material areas; areas with high-value objects or materials such as artwork, cash, drugs, confidential or historical documents, audiovisual and computer equipment and VIP areas.
- In some applications, video cameras can be used in combination with intercoms, telephones, or other entry control systems to provide for visual identification before granting entry to locked doors.

- In the future, Stanford may have a security operations center capable of monitoring a Video Surveillance System. At that time, Stanford will move to standard design principles and practices. Newly designed systems should support the standard for integration and future central monitoring functionality.

The following are control expectations:

- All Video Surveillance Systems at Stanford for security and safety purposes must be approved by the VSGG or its designee prior to installation.
- Access privileges to camera views and recorded video should be controlled and limited to as few authorized individuals as necessary.
- Implement maintenance for system components.
- Posting of video clips or still images to the Internet or for other public or private uses is forbidden including Facebook, YouTube, etc., unless reviewed and approved by the VSGG.
- Cameras should not be installed with the intent of recording computer screens without prior approval from the VSGG or for a criminal investigation.
- In general, Video Surveillance Systems at Stanford are primarily for forensics value for investigative purposes and not intended for constant, real-time monitoring of activities. Fixed-view cameras are preferred. Pan/Tilt/Zoom (PTZ) cameras may be used only when it is intended for cameras to be monitored by an operator in real-time.
- Fixed-view cameras are preferred. Pan/Tilt/Zoom (PTZ) cameras may be used only when it is intended for cameras to be monitored by an operator in real-time.
- Installation of cameras that are not recording (dummy) is prohibited in any and all cases on Stanford property. Dummy cameras intended as a deterrent can foster a false expectation of security and safety.
- Video in ATM machines managed by financial institutions is an exception.

Respectful Uses of Video Surveillance Systems

Video Surveillance Systems should not intrude unduly or unreasonably on the privacy interests of Stanford community members and guests.

- General video surveillance is not permitted unless otherwise detailed in these Guidelines. Covert video surveillance should be used only in rare circumstances for a specific security purpose, such as an investigation or protection of a particular area or activity. With the exception of DPS, VSGG approval is required for any covert video surveillance application.
- Stanford does not use Video Surveillance Systems for the purposes of workplace or workforce monitoring.
- Do not install Video Surveillance Systems where privacy interests exceed the security value.
- Do not record sound or speech as part of authorized Video Surveillance Systems. California law prohibits the recording of sound or speech without the consent of all parties involved.

Video Surveillance Procedures & Policies

Information obtained through Video Surveillance Systems will be used primarily for security, safety, and law enforcement purposes. However, Stanford reserves the right to use the information for other University purposes including but not limited to support of administrative or disciplinary proceedings against faculty, staff, or student(s), or in a civil suit against person(s) whose activities are shown on the recording and are the basis for the suit.

1. Video monitoring and recording for security purposes will be conducted in a professional, ethical, and legal manner. Violations of the procedures for video monitoring referenced in this policy will result in disciplinary action consistent with the rules and regulations governing Stanford community members.

2. Managers of Video Surveillance Systems will identify a Video Surveillance System administrator who will monitor and record based on suspicious activity or behavior and not individual characteristics. Video Surveillance System administrators will monitor and record in a manner consistent with all Stanford policies, including the Non-Discrimination Policy, the Sexual Harassment Policy, and other relevant policies. Camera control operators will not monitor and record individuals based on characteristics of race, gender, ethnicity, sexual orientation, disability, or other classifications protected by Stanford's Non-Discrimination Policies.

3. Camera control operators such as administrators, managers, and/or other individuals with authorization to operate Video Surveillance Systems will not seek out or continuously view or record people being intimate in public areas.

4. Camera control operators and/or managers of Video Surveillance Systems will not view or record private offices or living areas.

5. SUDPS, or any Stanford department or division with authorization by the Chief of Police and while under SUDPS management and control, is authorized to use Video Surveillance Systems to record events where there are likely to be violations of Stanford rules, regulations, policies, or violations of law. Cameras may be operated either overtly or covertly depending on the circumstances. In cases of demonstrations, protests, and similar situations, use of cameras, fixed or portable, will be generally overt, with the intent and purpose of deterring illegal acts.

6. Cameras may be permanently mounted or operated from a remote location or by an automated device. The following signage is required at locations where cameras are in use and must be conspicuous.
    - Cameras in Use – Not a Guarantee of Safety or Security
    - Cameras In Use

7. SUDPS shall determine which sign is required, if any, and where it must be posted at the time the application is approved.

8. The sign must include contact information (phone number or email address) for the authorized individual, department, or division responsible for the Video Surveillance System.

9. Individuals and departments who have received SUDPS or VSGG approval to operate and manage Video Surveillance Systems will make available to VSGG the recorded images or will permit access to their application via the Stanford network for maintenance, auditing, or investigations.

10. Recorded images will be stored in a secure location with access by authorized personnel only. The definition of a "secure" location for purposes of these Guidelines is a room or closet that is always locked with authorized access only by key or, preferably, a card reader.

11. Recorded images will be stored no less than 32 days (90 is recommended) and no more than 365 days, unless retained as part of a criminal investigation or court proceeding (criminal or civil), or other use as approved by the Chief of Police or designee. Quality of the video frame rate, camera placement, type, lighting, lensing, focus, view, and configuration should be designed to provide images of sufficient clarity and resolution to make an identification of individual faces and physical descriptions.

12. Only SUDPS, VSGG, Director of Compliance, Vice President of Business Affairs, General Counsel, or designee may release data produced by video security applications.

13. Each Stanford department or division with a Video Surveillance System must provide SUDPS with a list of individuals who can be contacted about the application during and after business hours, including weekends and holidays.

14. Installation of Video Surveillance Systems is the financial responsibility of the requesting departments and/or authorized individuals. This responsibility includes, but is not limited to, the cost of the system design, consultant fees, labor, installation, procurement of and connection to service, repairs, and maintenance. Fees are subject to approval by the Stanford recharge process.

To maintain an informed Stanford community, the VSGG will periodically disseminate written materials describing the purpose of Video Surveillance Systems and the guidelines for its use.

Video Surveillance - Workflow Responsibility Matrix

Project Phase	Land, Building, & Real Estate	Project Architect	Security Consultant	Public Safety / Risk	Zone Manager
Program	Budget	Budget Prep	Program Assessment / Design	Approve Security Program & Budget	
Schematic	Approve	Coordinate	Layout Security	Layout Security	Review
Design Development	Review/Approve	Design	Design Security	Design Security	Design Input
Construction Documents	Review/Approve	Plan Review & Coordinate	Design	Design	Design Input
30% Status	Review/Approve	Review/Approve	Design	Design	
60% Status	Review/Approve	Review/Approve	Design	Design	
90% Status	Review/Approve	Review/Approve	Design	Design	Design Input
100% Drawing/Spec	Review/Approve	Review/Approve	Finalize Design	Finalize Design	Approve
Project Management	Manage Security Contractor		Review		
Training/Document			Review/Approve	Review/Approve	Participate in Training
Pre-Test Approval			Review/Approve	Review/Approve	
Final Commissioning		Review/Approve	Review/Approve	Review/Approve	Review/Approve

Responsibilities

VSGG or Designee

- Review and approve existing and proposed Video Surveillance Systems at locations dictated by this policy.
- Monitor developments in relevant laws and in the security industry to assure that Video Surveillance Systems on Stanford property are consistent with the highest standards and protections.
- Maintain a list of Stanford owned, managed or controlled camera locations.
- Receive all requests for the release of recordings obtained through Video Surveillance Systems.
- Periodically review this policy and approves updates.

LBRE Capital Projects

- Coordinate with SUDPS to design and install Video Surveillance Systems in new construction and existing buildings. Capital Projects may not install a Video Surveillance System that has not been reviewed and approved by the VSGG or its designee.
- Incorporate Video Surveillance Systems into specific construction project budgets.
- When installing Video Surveillance Systems equipment on the exterior of a building, in the landscape, or in a public interior space, please review the proposed location and associated installation details and signage with Office of the University Architect/Campus Planning and Design.

Stanford Departments

- Departments with existing Video Surveillance Systems must have their applications reviewed by the VSGG or designee.
- Departments that wish to install new Video Surveillance Systems must submit their plans to the VSGG or designee for review and approval.
- Departments should carefully consider who may be viewing video monitoring and recording as judgment and ethical behavior are important relative to individual privacy concerns and applicable laws. Individuals acting as Building Managers have access to video monitoring.

Business Affairs Information Technology

- Oversight and responsibility of security integrator/contractor requirements for use of Stanford University's data network and network security.
- Maintain scheduled maintenance records of software versions and upgrades, as well as manufacturer patches and licenses.

Office of Risk Management & Office of General Counsel

- Provide counsel and advice on questions involving liability as well as moral or ethical issues.

Working with Video Surveillance System Guidelines

Program and Conceptual Design

- Identify building type and purpose, security basis-of-design, and any special requirements.

Schematic Design

- Convey security design intent, purpose, and basis of design to design team.
- Develop security narrative, outline physical security features and planned security electronic systems.
- Based primarily on CPTED strategies, coordinate major physical security elements, circulation zones and patterns, lighting, and exiting paths.

Design Development and Construction Documents

- Employ standard design templates with modifications as necessary or required.
- Incorporate security drawings and specifications into bid documents.
- Review and approval of Security Design Documents and Construction Documents.

Procurement and Construction

- Security shop drawings submitted, reviewed, and approved for compliance with construction documents, security design intent and purpose, and Video Surveillance Systems Guidelines.
- Installation, programming, and start-up coordinated with IT Services and SUDPS.
- Acceptance testing, commissioning, and approval of installation.
- Delivery and approval of as-built documentation.

Video Surveillance System Guidelines:

http://web.stanford.edu/group/SUDPS/docs/vssguidelines.pdf

For a Security Vulnerability Assessment and Sign Templates – Contact Bill Larson (SUDPS) at: william.larson@stanford.edu or (650) 725-2148