Stanford

Stanford University
Video Safety and Security Systems Standards

Revision Date: 5/31/2023
Effective Date: 4/18/2022

Video Safety and Security Systems Standards Statement

All Stanford University ("Stanford")[1] implemented and controlled video surveillance, monitoring, recording applications and installations ("Video Safety and Security Systems" or "VSSS"; may also be referenced as "cameras" in this document) must conform to the Stanford Video Safety and Security Systems Standards ("Standards") unless the Infrastructure Safety and Security Committee ("Committee") approves an exception. The Committee consists of representatives from the Stanford University Department of Public Safety (SUDPS); Office of the Chief Risk Officer (OCRO); Office of the General Counsel (OGC); Land, Buildings & Real Estate (LBRE), Graduate School of Business (GSB); Institutional Equity, Access & Community; Stanford Redwood City (SRWC); Stanford Health Care (SHC); University Privacy Office (UPO); Residential & Dining Enterprises (R&DE); Department of Athletics, Physical Education, and Recreation (DAPER); Stanford University Libraries (SUL); Environmental Health & Safety (EH&S); Office of the Vice President of the Arts (VPA); Office of the Vice Provost for Student Affairs (VPSA); and University IT (UIT). Except as provided in these Standards, VSSS will not be used to view, monitor, or record private spaces (as further described in these Standards). However, nothing in these Standards prevents the use of VSSS in connection with an active criminal investigation or lawful request or court order. The Committee reserves the right to review and approve any proposed or existing VSSS on properties owned, leased, managed, or controlled by Stanford.

Guiding Principles of Security and Privacy

Stanford recognizes that VSSS plays a significant role in maintaining safety and security on campus – but also that video monitoring can sometimes be in tension with individual expectations and rights to privacy. Accordingly, in developing and implementing these Standards, a variety of potentially competing interests must be considered and balanced. For example, Stanford typically deploys video cameras at targeted, high-risk locations where there is an increased potential for crime, rather than blanketing the campus with ubiquitous video surveillance – which would undesirably chill creativity and freedom of expression and profoundly change the campus environment for our faculty, staff, students and visitors. As a guiding principle, these Standards are intended to facilitate effective deployment and management of VSSS for the safety and security of our community, in a way that is also consistent with Stanford's commitment to protecting privacy.

Design Principles and Practices

The intent of these Standards is to establish an approved guide for the design, use, placement/installation, operation, and maintenance of VSSS. The VSSS are a component of a comprehensive and integrated approach to safety and 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 company resources.

To ensure the forensic value of the data, any VSSS installed after the approval of this Standard must be compatible with the Stanford enterprise access system, the UIT procedure for access, and accessible to SUDPS.

SUDPS must perform a Security Vulnerability Assessment ("Assessment") for each VSSS project as a part of the design process. The Assessment consists of a review of the physical security and security policies and procedures, signage requirements, secure location of recorded images, and a review of adherence to Stanford's Minimum Privacy Standards (in coordination with UPO, as appropriate). The Committee may evaluate the findings and suggestions included in the Assessment, and may require them to be incorporated into the system design. Quality of the video frame rate, camera placement, type, lighting, lensing, focus, view, and configuration shall be of benefit to an investigation and be designed as part of the Assessment to provide images of sufficient clarity and resolution to make an identification of individual faces, physical descriptions, and vehicle descriptions (including license plates).

[1] These Standards only cover the use of video technology for the purposes of monitoring for safety, security and law enforcement, and limited incidental purposes. Other uses of video technology at Stanford are beyond the scope of these Standards.

Administration and Implementation

The Committee administers these Standards. SUDPS is charged with reviewing, suggesting, and approving, proposed and existing VSSS applications, in compliance with these Standards. SUDPS is available to discuss and review security programs and operations with Stanford building managers, zone managers, project managers, department heads/chairs, and managers of tenant-operated facilities and programs.

Scope of Standards

- Any Stanford department, school, unit or division that uses VSSS for the purpose of safety or security in any location owned, leased, managed, or controlled by Stanford.
- Planners, architects, designers, vendors, and contractors for all construction projects at Stanford.
- Internal Stanford users, and lease tenants on Stanford property that are incorporated into university operations.
- Stanford as a tenant; Stanford will negotiate the appropriate requirements with landlords to the extent possible.
- The following sites are out of scope of these Standards: ground leases where a third-party occupies buildings on Stanford property but there are no university operations; Stanford hospitals; campus residence leaseholders; and food, lodging, and retail operations that are not a part of university operations. For food, lodging, and retail operations that are not a part of university operations, the entity entering into the agreement on behalf of the university shall take into consideration as part of the agreement the university's expectations for camera monitoring, recognizing both the intent of these Standards as well as concerns of the involved entities.
- VSSS installed prior to the establishment of these Standards (April 2022) are still expected to be in compliance with the values, policies, and procedures documented in these Standards, to the extent technically possible.
- Departments and schools with existing VSSS must have their systems reviewed by the Committee for compliance to these Standards at time of refresh, renovation, or new construction.

Value Expectations

Security systems, including VSSS, are intended to assist in mitigating risk to people, property, and the educational, institutional, and operational processes at Stanford. The systems can provide the following security and safety features:

- VSSS may serve as a crime deterrent.
- Once a crime has been committed, the systems may assist in identifying the responsible parties.
- Video monitoring 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 VSSS at Stanford is to record activity of building entrance and exit points, perimeter doors, intersections, parking structures, and parking lots. Building interiors in immediate proximity to entrance and exit points (e.g., office and lab facility lobbies), and other high-risk areas as described below, may be monitored by VSSS. However,

monitoring of student lounges, dining rooms, and other living areas within student residences are not permitted under these Standards.

- VSSS may target areas (whether inside or outside buildings) deemed by SUDPS or the Committee to be high-risk, including certain types of laboratories; mission-critical buildings such as data centers and energy facilities; large venues such as stadiums, arenas, theaters; hazardous material areas (including chemical, biological, and gas storage areas); areas with high-value objects or materials such as artwork, cash, pharmaceuticals, confidential or historical documents, audiovisual and computer equipment, VIP/Dignitary areas, retail establishments and other areas where safety or security-related transactions between Stanford personnel and patrons or visitors may raise heightened safety or security concerns (e.g., checkout areas and bag check desks at Stanford libraries). High risk areas and other parameters will be defined in the Assessment completed for each VSSS project as part of the design process.
- VSSS may be used in combination with intercoms, telephones, gates, or other entry control systems to provide for visual identification before granting entry to locked doors.
- The University does not currently use VSSS to record speech or sound, and has no plans to do so as of the effective date of these Standards. However, the Committee may in the future amend these Standards to allow for speech or sound recordings in narrowly tailored circumstances (to be described in the amendment); provided, however, that any future proposed recording of speech or sound must be consistent with each of Stanford's Minimum Privacy Standards (https://minpriv.stanford.edu), the criteria set forth in the Guiding Principles for the Use of Sensors on Campus (https://privacy.stanford.edu/guidelines/guiding-principles-use-sensors-campus), and applicable law, as determined by OGC and UPO.
- VSSS are intended to be used for forensics; however, it may also be used for live monitoring in furtherance of physical safety and security, such as for traffic or crowd management, including during stadium events, or a serious crime in progress (such as an active shooter) or a significant threat to public safety (such as a fire or explosion).

Respectful Uses of VSSS

VSSS shall not intrude unduly or unreasonably on the privacy of Stanford community members and guests.

- Continuous, routine live monitoring (instead of passive recording) is not permitted unless otherwise detailed in these Standards.
- VSSS shall not be used for monitoring individual students, employees, or members of the general public unless there is evidence or reasonable suspicion that criminal activity is occurring.
- Only SUDPS may approve of any lawful covert video monitoring application controlled by the university.

Video Monitoring Policies & Procedures

Sole Purpose of VSSS Installations and Video Capture: VSSS may be installed solely for safety, security and law enforcement purposes – and for no other purpose.

Primary and Secondary Uses of VSSS Recordings: Video recordings and related information obtained through VSSS will be used primarily for safety, security and law enforcement purposes. ("Primary Purpose"). However, from time to time, video recordings incidentally captured (during the course of the primary use of VSSS) may be used for a secondary purpose of supporting litigation or an investigation or proceedings related to an alleged violation (based on reasonable suspicion) of a legal requirement, the Stanford Administrative Guide, Stanford Bulletin, Title IX, SHARE, Honor Code, Fundamental Standard, Student Group Accountability Process, Code of Conduct, Research Policy Handbook involving Stanford faculty, staff or student, or any other policy, rule, or regulation to which Stanford faculty, staff, or students are subject. ("Secondary Purpose"). Except as described above, video recordings will not be used for the purpose of tracking daily performance, attendance or location of individual Stanford students, faculty or staff.

1. Video monitoring and recording for security purposes will be conducted in a professional, ethical, and legal manner. Violations of the requirements referenced in these Standards may result in disciplinary action consistent with the rules and regulations governing Stanford community members, as documented in the Stanford Administrative Guide.

2. All VSSS at Stanford for security and safety purposes must be approved by the Committee or its designee via the VSSS request process and comply with the Workflow Responsibility Matrix contained within this document as well as with the most current Facility Design Guideline (FDG) available at the time of design. Video doorbells are not permitted as they do not comply with these Standards. When existing video doorbell installations are identified, SUDPS will request that they are removed. Approval of exceptions or alternatives will require approval of the Committee.

3. Managers or owners of VSSS will identify a VSSS administrator or manager who will

use and administer the system in accordance with the VSSS Standards based on suspicious activity, criminal activity or behavior, and not based upon individual characteristics; list of sites, camera locations, and contacts to be maintained by SUDPS. VSSS administrators or managers will monitor and record in a manner consistent with all Stanford policies, including but not limited to the Non-Discrimination Policy, the Sexual Harassment Policy, Minimum Privacy Standards, and other relevant policies and procedures. 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.

4. Operators must be trained on the proper use of the systems, in accordance with these Standards.

5. Camera control operators such as administrators, managers, and/or other individuals with authorization to operate VSSS shall not seek out or continuously view or record intimate or other private, lawful activity.

6. VSSS will not be installed or used to record in (a) the interior of buildings, except as specifically permitted in these Standards, (b) student, faculty or staff living areas, (c) restrooms, (d) lactation rooms, and (e) any other area where faculty, staff, students or visitors have a reasonable expectation of privacy. VSSS shall not be used to generally monitor students or personnel.

7. Cameras will not be installed with the **intent** of actively monitoring or recording computer screens without prior approval from the Committee, the Dean of Research's Office for certain experiments/research, or for a criminal investigation. The exception may be for research to monitor an experiment or to monitor equipment operation (e.g., to check for flooding or machinery failure).

8. SUDPS, or any Stanford department, school, division or unit is authorized to use VSSS to record events or specific incidents for safety and security purposes where there are reasonably likely to be violations of Stanford rules, regulations, policies, or violations of law. Any recording of an event or incident, whether covert or overt, in conflict with any parameter of the VSSS Standards must request an exception prior to recording; exceptions can be authorized only by SUDPS and OGC.

9. Cameras may be permanently mounted or operated from a remote location or by an automated device.

10. Fixed-view cameras are preferred. Pan/Tilt/Zoom (PTZ) cameras should be used only when it is intended for cameras to be monitored by an operator in real-time.

11. Installation of cameras that are not recording (dummy cameras) or leaving cameras up that are known to no longer be functional is prohibited; non-functioning cameras must be removed or covered while awaiting repair or replacement. Additionally, signage regarding cameras must not be posted where there is not the placement of functioning

cameras.

12. Although the specific location of cameras need not be disclosed to individuals, reasonable notice must be provided regarding use of VSSS, in accordance with Stanford's Minimum Privacy Standards (this includes cameras that are not under the scope of these Standards). One of the following signs, as applicable, is required at locations where cameras are in use and must be conspicuous:

    Cameras In Use – Not a Guarantee of Safety or Security (e.g., labs, gyms/pools)
    Cameras In Use (Building interiors)
    Cameras In Use On These Premises (Building exteriors; most buildings and facilities post this sign)

    The sign must include contact information (phone number or email address) for the authorized individual, department, school, division or unit responsible for the VSSS.

    Depending on the number and location of entrances to a building or venue, multiple signs may be required to appropriately notify individuals.

13. Individuals and departments who have received SUDPS approval to operate and manage VSSS will make available to SUDPS or the Office of General Counsel the recorded images or will permit access to their application via the Stanford network for maintenance, auditing, or investigations. Requests that involve third-parties will be evaluated on a case-by-case basis, as they may require a warrant or subpoena.

14. Recorded images will be stored in a secure location with access by only as few authorized personnel as necessary. A secure location is defined as a room, closet, cabinet or cage that is controlled by 24/7 card or key access. Going forward, Stanford will transition to a cloud-based platform, and images will be stored within encrypted cloud storage infrastructure. Stanford will deploy local, on-premises gateways to cover approximately three days of storage if the connection to the cloud is disrupted. Gateways will be housed in secured data centers or ECH locations.

15. Recorded images will be stored no fewer 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), in response to a litigation hold issued by the Office of General Counsel, or for other uses as approved by the Chief of Police or his/her designee.

16. Access privileges to camera views and recorded video will be controlled and limited to as few authorized individuals as necessary, and only to those with a legitimate purpose to access video footage; and such individuals will be granted access only to the specific, minimum video footage necessary to achieve such purpose(s). SUDPS will have access to all VSSS and use that access as appropriate to support investigations and emergencies. SUDPS and UIT must be notified when there is a change of a VSSS administrator or manager.

17. Posting of video clips, URLs, or still images to the Internet and any other sharing to

unauthorized individuals by any medium (e.g., printing out still images and sharing or sending video files to unauthorized individuals) or for other public or private uses is forbidden unless reviewed and approved by the Committee.

18. Only SUDPS, the Office of General Counsel, or a designee may release data produced by video security applications (extracted by UIT). The chain of custody with reference to the video footage in question will be ensured to prevent tampering or manipulation of any sort.

19. Any outside agency that requests video to assist with an investigation must serve a subpoena or warrant to the OGC; an exception can be made in an active or in progress threat situation for which SUDPS or the OGC can approve an exception.

20. Installation of VSSS is the financial responsibility of the requesting departments, schools, units, divisions, and/or authorized individuals. This responsibility includes, but is not limited to, the cost of the system design, consultant fees (if applicable), labor, installation, programming, procurement of and connection to service, signage, repairs, removal, and maintenance. In the event that a camera project qualifies for and is prioritized for deployment, central funding may be available for installation and refresh, but the requesting department would be responsible for covering ongoing operational expenses.

21. Departments, schools, or units who own the VSSS will maintain their systems with recurring reviews to ensure cameras are operational and are meeting functional requirements. Any VSSS not functioning properly must be reported to SUDPS and UIT in a timely manner (i.e., no later than 2 business days after the VSSS administrator learns of a malfunction). A certified and licensed technician will complete an annual inspection of all electronic equipment; all costs borne by the respective system owner.

22. Stanford recognizes that facial recognition and similar technologies may provide security benefits of enhanced identification, but may also present meaningful risks related to privacy, inaccuracy, and racial and/or other bias that are inconsistent with Stanford's policies and values. Stanford does not use facial recognition or similar technologies on video footage collected under these Standards; and such activities are not permitted under these Standards, except as described below.

    From time to time in the context of a government investigation, the University may be required to provide selected video footage collected under these Standards to law enforcement; and law enforcement may subsequently use facial recognition or similar technologies beyond Stanford's control. In such circumstances, to the extent practicable and allowable (e.g., if not compromising an ongoing investigation), Stanford will (1) work with law enforcement to determine how such facial recognition or similar technologies will be or have been used, and (2) notify affected individuals of such use, when feasible and known to the university.

23. Any access or use of video recordings for a Secondary Purpose must be approved in advance by a representative of each of OGC and UPO, and one Authorizing Official, who together must (a) make a factual determination that the legal proceeding or allegation has a sufficient basis to support access and use, and (b) weigh the need for access and use against other University concerns, including academic freedom, personal privacy, integrity of University operations, compliance with law and policy, protection of life and property, and determine that the access and use of the video recording(s) will advance a legitimate institutional purpose and that such need outweighs any countervailing considerations. For purposes of these Standards, an "Authorizing Official" means an Associate Vice President for Human Resources (for employee matters) or the Vice Provost for Student Affairs (for student matters), or her or his designee.

24. Video recordings unrelated to safety and security are outside the scope of these Standards, including video captured:
    1) In classrooms, conferences or seminars for educational or discussion purposes,
    2) In labs for research and equipment operation purposes,
    3) Athletic training, and
    4) At Stanford event venues, in furtherance of the event (e.g., for entertainment or hospitality purposes).

    Stanford University facilities that are supported by Stanford Medicine Security should endeavor to follow these Standards in collaboration with SUDPS.

    In addition, video captured at ATM machines or similar kiosks (e.g., parcel lockers) are covered by separate policies and requirements outside the scope of these Standards.

Any updates to these Standards must be reviewed and approved by the Executive Steering Committee (ESC) of the Infrastructure Safety and Security Committee.

Additionally, any proposed updates to the Standards related to facial recognition or similar technologies would be subject to approval by the President, with input from the Faculty Senate Committee on Academic Computing and Information Systems (C-ACIS), the Executive Steering Committee, and the University Privacy Office. Such updates must also be consistent with Stanford's Minimum Privacy Standards (minpriv.stanford.edu) and the criteria set forth in the Guiding Principles for the Use of Sensors on Campus (https://privacy.stanford.edu/guidelines/guiding-principles-use-sensors-campus).

To maintain and inform the Stanford community, the Committee will post any updates to the Standards on the University IT website.

Responsibilities

Video Monitoring Workflow Responsibility Matrix [1]

Project Phase	Dept. or School	Project Manager	Security Consultant (if applicable)	SUDPS and / or Committee	Building or Zone Manager
Project Initiation	Submit Form-1	Develop ROM Budget	N/A	Confirm VSSS Standards (FDG)	Informed of project
Scoping / Programming	Define Program Reqs.	Lead Scoping	N/A	Define Tech. Reqs.	Resource
Schematic Design (SD Phase)	Confirm Program Reqs.	Lead SD	Design	Review	Resource / Review
Design Development (DD Phase)	Confirm Design Meets Program Reqs.	Lead DD	Develop Design	Review	Resource / Review
Construction Documents (CD Phase)	N/A	Lead CD	Finalize Drawings	Review	Resource / Review
Training / Document	Participate in Training	Set Up / Document Training	Conduct Training	Participate as required	Participate in Training
Pre-Test Approval	N/A	Coordinate Pre-testing	Conduct Pre-test	Approve testing docs	Participate
Final Commissioning	N/A	Review / Approve / Distribute	Conduct Commissioning	Accept / Ownership	Accept / Ownership

[1] For specific areas of campus that are not necessarily owned by one school or department, a unit with a stake or interest in a particular area may propose or initiate a project.

Committee

- Review and approve existing and proposed VSSS at locations dictated by this policy.
- Monitor developments in relevant laws and in the security industry to assure that VSSS on Stanford property are consistent with current industry standards and legal requirements. Verify that all systems meet these Standards and guidelines set forth in the Stanford Administrative Guide.
- Maintain a list of Stanford owned, leased, managed, or controlled camera locations.
- Review and update these Standards on an annual basis.

LBRE and R&DE Capital Projects

- Coordinate with SUDPS to review the design of, or revisions to, VSSS in new construction and existing buildings. Departmentally Managed Projects may not install a VSSS that has not been reviewed and approved by the Committee or its designee.
- Where VSSS is approved, incorporate VSSS into construction project budgets as required.
- When installing VSSS equipment on or around the exterior of a building, an outside public space, or in a prominent interior space, the Office of the University Architect/Campus Planning shall review the proposed camera locations.

Stanford Departments and Schools

- Departments and schools with existing VSSS must have their systems reviewed by the Committee for compliance to these Standards at time of refresh, renovation, or new construction.
- Upon approval of VSSS implementation; departments or schools must submit their plans to the Committee for review and approval.
- Departments or schools 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 authorized to access video monitoring must follow the policies and procedures in these Standards.

University IT (UIT)

- Oversight of the installation, operations, and maintenance of VSSS.
- 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.
- Updating FDGs for VSSS.

Office of Risk Management, Office of General Counsel, University Privacy Office

- Provide guidance involving potential liability as well as privacy issues. Advise in instances of litigation, threatened litigation, or government

investigations.

Implementation of Video Monitoring Systems (by Phase)

Scoping and Programming

- Define program and technical requirements to determine the scope of the system being designed.
    - Consider building type and purpose.
    - Conduct a Security Vulnerability Assessment.
    - Determine any special requirements based on building use/type or user needs.
    - Develop security basis-of-design, narrative and specifications.

Schematic Design and/or Design Development

- Review and develop security design intent, purpose, and basis of design with the design team.
- Identify purpose or intent, outline physical security features, and planned security electronic systems.
- Utilize CPTED strategies and industry standards to coordinate physical safety and security elements, circulation zones and patterns, lighting, and exiting paths.
- Employ standard design templates with modifications as necessary or required.
- Review and approval of Security Design Documents for compliance with construction documents, security design intent, and purpose, and VSSS Standards.

Construction Documents

- Incorporate security drawings and specifications into construction bid documents.
- Submit for any required permits.

Construction and Turn Over

- Installation, programming, and start-up coordinated with UIT and SUDPS.
- Acceptance testing, commissioning, and training.
- Delivery and approval of as-built documentation.
- Submission of drawings, including floor plans with camera locations, to Maps and Records.

For a Security Vulnerability Assessment and Sign Templates, contact Bill Larson (SUDPS) at: **william.larson@stanford.edu.**