Title of University Executive Directive: Electronic Security System
University Executive Directive #25-47

Recommended By: (The Cabinet where the University Executive Directive was developed.)	University Police Department, Information Technology Services, Facilities Services and Procurement & Support Services
Contact Information: (Position Title / Contact Name / Contact phone number / Contact Email)	Assistant Vice President for Campus Safety & Chief of Police Reginald D. Parson regg@sfsu.edu 415 338-2747 Sr. Assistant Vice President & Chief Information Technology Services Nish Malik nish@sfsu.edu 415 338-1133 Assistant Vice President Capital Planning Design Construction & Facilities Services Barry Jodatian Jodatian@sfsu.edu 415 338-1568 Interim Procurement & Support Services Director Steven Chang stevenchang@sfsu.edu 415 338-2547
Effective Date: (When the Policy was enforced.)	____, 2025
Revised Date: (When the Policy was last edited or revised.)	

Final Draft

I. Authority (i.e., Executive Order, ICSUAM, Delegations of Authority):

Within a broad context, the university stakeholder departments (i.e. University Police Department, ITS, Facilities Services and Procurement & Support Services) are each charged with the following agenda:

[1] YY signifies the year in which the University Executive Directive was enacted.
[1] NN signifies the number of the University Executive Directive, which are listed consecutively.
For assistance, please contact the Audit & Policy Coordinator at policies@sfsu.edu.

- Providing centralized core of expertise and assistance to departments, program centers and others in electronic security design and development;
- Ensuring that the systems acquired are high quality products, designed and functioning to meet security objectives with longevity in mind;
- Providing technical procedures, standards, monitoring processes and coordination for managing the design, acquisition and construction of security systems;
- Establishing operational procedures and protocols for monitoring and responding to an "alarm" condition whether reported locally or remotely via a third-party service bureau;

All actions representing this policy and the activities performed under its provisions are assigned to the Office of the Vice President for Administration and Finance.

II. Purpose:

This Directive establishes a consultative review process by which the department may, after approval, establish electronic monitoring, intrusion, panic or status alarm services housed on campus or at officially designated off-campus sites. A secondary goal is to develop a framework to ensure that all electronic alarm systems comply with San Francisco State University Information Technology Service (ITS) standards, electrical and building codes, Human Resource standards, collective bargaining agreements as well as the University Police Department operational procedures and systems.

The execution of this policy ensures an institutional perspective that guarantees that all electronic alarm systems will be technologically and operationally integrated into the University Police Department and campuswide functions.

III. Policy Statement:

A university of such size and scope as San Francisco State University, and with a commitment to preserving an open access environment for students, faculty, staff and the general community, faces unique security obligations. The development of any security plan necessitates consultation

with the University Police Department, since any action taken requires a centralized response. Security controls employing electronic monitoring, intrusion systems, emergency phones, panic or status alarm services can be designed to meet an array of security goals but must be aligned with overall security plan for the campus. Regardless of design or functionality, each system must meet the operational and technological standards that will allow the University Police Department to integrate it successfully into centralized operational and/or physical infrastructure of the campus.

a. Who This Policy Applies To:

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

Final Draft

[1] YY signifies the year in which the University Executive Directive was enacted.
[1] NN signifies the number of the University Executive Directive, which are listed consecutively.
For assistance, please contact the Audit & Policy Coordinator at policies@sfsu.edu.

b. Obligations of Departments:

It is the responsibility of the department to provide the necessary funding required to design, install, maintain and support monitoring and/or status service (if provided by other than the University Police Department). Security system compliance with said policy shall include all present facilities and any newly developed projects set forth hereafter. Any electronic security system and/or electronic monitoring system, whether generating a local alarm, transmitting an alarm condition to a third-party service bureau or centrally to the San Francisco State University Police Department, is governed by this policy.

c. Obligation of Others:

The University Police Department, Facilities Services, and Capital Planning, Design and Construction are assigned the functionality and responsibility of assisting departments, program centers or others in the assessment and development of electronic security services. Charges for providing these services are applied only as approved by the San Francisco State Cost Recovery Oversite Committee.

i. University Police Department
- Security assessment, planning and review
- Security hardware system design and service evaluation
- External consultant engagement and security services availability
- University Police Department monitoring and protocol standards
- Liaison for third party organizations and individuals
- University Police Department hardware/software interoperability requirements

ii. Information Technology Services (ITS)
- System design, equipment lists and bid specifications
- Equipment, hardware assessment and compliance
- Installation and performance testing of third-party systems
- ITS installation/construction and coordination services
- Interoperability monitoring and compliance with telephone or radio communication rules and regulations

iii. Facilities Services
- Installation and construction logistics and scheduling coordination
- Vendor compliance with local/state/university/architectural/electrical/fire codes
- Installation and specification of related signage

iv. Procurement & Support **Services**
- Bid specification and processes
- Bid assessment and acquisition services
- Vendor and contractual obligations
- Compliance requirements and services

[1] YY signifies the year in which the University Executive Directive was enacted.
[1] NN signifies the number of the University Executive Directive, which are listed consecutively.
For assistance, please contact the Audit & Policy Coordinator at policies@sfsu.edu.

Final Draft

IV. Procedures (hyperlink):

The design and implementation of an electronic security system can vary dramatically. Each system is therefore customized or tailored to meet specific objectives of the department or program center. As a general guideline, placement of security alarm and monitoring systems should be justified using the following criteria to assess need:

1) Life safety;
2) Property security;
3) Cash and sensitive material handling;
4) High profile areas (i.e. frequent dignitary visits), criminal or incident activity patterns;
5) Traffic safety.

To assist in defining these objectives, the initiating department should meet with the University Police Department and ITS. Unique applications may also require engaging a security consultant. Conclusions reached by the University Police Department and ITS, the initiating department and consultant shall present a proposal requiring approval by the department's and/or the program unit's senior level administrator.

Security hardware, operational procedures, and alarm services, shall be reviewed and approved by the University Police Department.

Warning and/or alert signage with appropriate language as required, shall be reviewed and approved by the Facilities Planning Committee and University Police Department.

Equipment, shall be reviewed and approved by the Information Technology Service's (ITS). Installation, signage and construction specifications shall also be reviewed and approved by ITS and Facilities Services.

Installation of systems shall be done in accordance with Federal, State and Local laws, codes and regulations.

The responsibility for procurement of equipment, installation and/or services shall be managed by Procurement & Support Services.

a. Video Security Cameras

San Francisco State adheres to and abides by the CSU Systemwide Video Security Camera policy, which can be found at the following link: https://calstate.policystat.com/policy/8020972/latest.

San Francisco State also adheres to and abides by the Federal guidelines governing the use of banned devices on state property and/or associated with state use. A full list of banned devices can be found at the following link: List of Equipment and Services Covered by Section 2 of The Secure Networks Act I Federal Communications Commission

[1] YY signifies the year in which the University Executive Directive was enacted.
[1] NN signifies the number of the University Executive Directive, which are listed consecutively.
For assistance, please contact the Audit & Policy Coordinator at policies@sfsu.edu.

Final Draft

Definitions:

- **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.

- **Video Security Camera**
  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.

- **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.

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

- **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.

Final Draft

President Lynn Mahoney Date

[1] YY signifies the year in which the University Executive Directive was enacted.
[1] NN signifies the number of the University Executive Directive, which are listed consecutively.
For assistance, please contact the Audit & Policy Coordinator at policies@sfsu.edu.