Security Systems

Original Implementation: July 20, 2010
Last Revision: April 20, 2021

Purpose

Stephen F. Austin State University is committed to the security and safety of our students, employees and visitors. This policy contributes to the fulfillment of that commitment and outlines how security systems are requested and maintained with the goal of standardizing components and processes. Stephen F. Austin State University adopts the university information security program along with other applicable governing regulations pertaining to the protection of the information collected as part of this policy.

Definitions

Access control systems enable the monitoring and control of access to facilities and resources. In the context of physical security, these systems record the request for and subsequently allow or deny access to the requested area or resources. These systems may include but are not limited to: access card, numeric code, biometric identification or proximity device for access.

Hold-up and Panic Alarms are devices that signal the University Police Department (UPD) of an event in which the personal safety of a member of the university community is in jeopardy. No on-site audible or visual signal is present in such applications. Locations where such systems could be installed include but are not limited to locations an armed robbery could be a threat or where staff may be subject to personal jeopardy.

Physical Intrusion Detection Systems are commonly referred to as “burglar alarms” and generally consist of door contacts, motion detectors, and glass breakage sensors. When these devices are triggered they signal a control panel to activate both an on-site audible alarm as well as register an alarm at the UPD dispatch communication center.

Security Camera Systems are devices designed to transmit video and/or audio signals to a monitoring station or recording device. The use of security cameras is generally for purposes of monitoring property subject to theft and supervising sensitive access points or offices/areas subject to disruptive behavior. No department is permitted to install any type of security cameras with the exception of UPD. These systems must be configured to be continuously monitored or recorded. "Dummy" security cameras are not permitted.

Security Systems as used in this policy is defined as any singular system or any combination of the systems defined above.

General

All security systems must be approved by the executive director /chief of police, or his/her designee and the appropriate vice president, or president's designee, prior to purchase and installation. Necessary approvals must be provided to Procurement and Property Services prior to orders being placed.

In facility construction and/or renovation planning, all included security systems must be approved by the executive director/chief of police or his/her designee prior to approval of final plans.

Upon installation of a security system, UPD will monitor the system for functionality at no cost to the installing department. Stand-alone security systems (those not monitored by UPD) are prohibited.

Security systems are installed for the protection of our students, employees and visitors. Therefore, security systems may not be removed, relocated, or modified without approval of the executive director/chief of police, or his/her designee

Protection of Recordings

For the purposes of security and potential evidence gathering, it is important that any audio or video recorded from security systems be protected.

Any department that has video and/or audio surveillance equipment installed shall provide the UPD with the appropriate authorization to view, download, capture, monitor, and control this equipment. This enables the UPD to maintain a chain of custody regarding evidence recovered from the recording device.

While the UPD will be responsible for the administration of all security system equipment, departmental directors and/or other authorized employees within each department with video and/or audio surveillance equipment installed may have authorization to view footage for non-security purposes.

An individual that accesses suspected criminal or suspicious activity should contact the University Police Department immediately.

Retention of Security Camera Recordings

Security camera recordings should be retained for a period of no less than 14 days. If existing systems do not provide for a storage period of that length, the maximum storage period possible should be utilized.

Cross Reference: Information Security Management (14.1)

Responsible for Implementation: Vice President for Finance and Administration

Contact For Revision: Executive Director/Chief of Police

Forms: Work Request form available on the UPD website

Board Committee Assignment: Building and Grounds Committee