Security Systems

Original Implementation: July 20, 2010
Last Revision: April 24, 2018

Stephen F. Austin State University has a commitment 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 security system components and processes as much as possible. 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 Controls

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

These systems are devices that signal the Department of Public Safety (DPS) 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

These are systems 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 DPS central monitoring station.

Security Camera Systems

These 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 DPS. These systems must be configured to be continuously monitored or recorded. "Dummy" security cameras are not permitted.

Security Systems

The term “security systems” as used in this policy is defined as any singular system or any combination of the systems defined above.

APPROVAL AUTHORITY

All security systems must be approved by the executive director of public safety/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 of public safety/chief of police or his/her designee prior to approval of final plans.

SYSTEM MONITORING

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

PROCEDURE FOR REMOVAL OR MODIFICATION OF A SYSTEM

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 of public safety/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 Department of Public Safety with the appropriate authorization to view, download, capture, monitor, and control this equipment. This enables the DPS to maintain a chain of custody regarding evidence recovered from the recording device.

While the DPS 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 Department of Public Safety 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 University Affairs

Contact For Revision: Executive Director of Public Safety/Chief of Police

Forms: Work Request form available on the DPS website

Board Committee Assignment: Building and Grounds Committee