SECTION: Campus Safety **Number: 06.06.01**
AREA: Security Technology

SUBJECT: Security Technology Systems

I. PURPOSE AND SCOPE

This documentation sets forth procedures which establish standards over the design, installation, function, registration and operation of electronic security systems within the facilities of the University of Houston.

II. POLICY

This policy applies to all facilities owned, leased, and/or under the control of the University of Houston. Any electronic security systems controlled by, reporting to, or that in any way communicates with the University host systems or monitoring facilities are subject to the requirements set forth herein. This policy shall apply to any and all security technology systems, including but not limited to electronic access control, security camera, security alarm and Code Blue Phone systems. After December 14, 2017, new system installations and any alterations to existing systems must be fully compliant with the provisions of this policy. The University of Houston Security Systems Review Committee may recommend exceptions or variations in the application of this policy on a case-by-case basis.

Electronic fire alarm systems installed as part of the University's fire alarm monitoring and control system are not subject to the provisions of this policy. Mechanical access systems such as mechanical code-operated locks are not governed by this policy. Alarms on research equipment such as freezer alarms are not governed by this policy.

III. DEFINITIONS

A. Electronic Access Control – Access control includes any electronic system that uses a code, card, device or biological characteristic of an individual as the basis for determining authority to gain entry to a facility. It does not refer to any other device that controls, inhibits or moderates traffic flow into and out of an area or building, including cut keys.

B. Security Camera Systems – Includes any video recording system that will accommodate the viewing of live or recorded video images for the purposes of criminal deterrence, detection or forensics investigations by the UH Police Department (UHPD). This policy does not include systems used for academic research, marketing, or management applications.

C. Security Alarm Systems – Security Alarm systems shall include all electronic systems installed for the purpose of detecting unlawful or illicit entry or access to college structures and buildings, and as well as for the remote transmission and annunciation of a signal of duress.

D. Code Blue Phones – Code Blue Phones are communications kiosks located on open areas of University grounds, including walkways, courtyards, parking lots, parking garages and the campus at large, as well as some designated areas within buildings. These devices provide a direct line of communication with UH police dispatch services in the event of emergencies.

IV. SECURITY SYSTEMS STANDING COMMITTEE

This policy establishes a security systems review committee which is responsible for the implementation and administration of the provisions of this policy.

A. The Security Systems Standing Committee (Committee) will consist of representatives from the following areas:

1. Campus Safety;

2. University of Houston Police Department (UHPD);

3. University Information Technology (UIT);

4. Facilities/Construction Management (F/CM);

5. Student Housing and Residential Life (SHRL);

6. Division of Research (DOR), and

7. Faculty Senate.

NOTE: Additional committee members may be appointed temporarily as deemed appropriate by the Committee.

B. The Committee shall meet as often as necessary, but at least once during each summer for an annual review of this policy.

V. DESCRIPTIONS OF ELECRONIC SECURITY SYSTEMS

A. All electronic security systems within the scope of this policy fall into sub-system categories. These sub-system categories include, but are not limited to:

1. Access Control;

2. Video Surveillance;

3. Security alarms, and

4. Code Blue Phones.

B. This policy defines the mandatory architecture for each of these distinct systems to which all proposed systems must comply. Wherever possible, proposed installations shall be integrated with other sub-systems or be consistent with their eventual integration.

VI. SYSTEM STANDARDS

The Committee shall establish minimum standards and requirements for the installation and operation of access control, video surveillance, code blue phones and security alarm systems. The minimum standards will be developed with growth, compatibility, maintenance, and response procedures in mind.

VII. STANDARDS REVIEW

The Committee will review systems standards to ensure ongoing compliance with business needs and to address the emergence of new technologies and their suitability for operational deployment.

VIII. ELECTRONIC ACCESS CONTROL

A. All electronic access control system installation and design shall be approved by Campus Safety (CS). Design Guidelines and Standards can be found in Section B2030 (Exterior Doors) and Section B2031 (Interior Doors) of the University of Houston Campus Design Guidelines and Standards, Construction Systems and Assemblies Standards and Guidelines.

B. All systems must comply with NFPA 101 and be able to integrate with the campus security camera network. Each department or business unit will adopt and implement this policy and follow the Electronic Access Control department guidelines related to electronic access and the issuance of metal keys to all exterior doors.

C. Campus Safety is responsible for the operational management of the central access control system. The system shall consist of a central control host server and remote building control panels, the associated readers and other peripheral devices. All system components shall be controlled by the central host via a communication network. Integration with the central control and monitoring system is mandatory for all installed systems. All access control system installed shall be functionally compatible with the University ID card.

D. The Committee may grant exceptions when deemed appropriate; however, stand-alone security systems are strongly discouraged. Independent access systems may be installed only after testing, review, and approval of system plans, specifications, designs, proposals, bids and/or quotes. Independent stand-alone systems **must** be able to integrate with other security systems (I.e., Camera System) used by Campus Safety.

E. Department justification for an autonomous stand-alone system cannot be based upon cost factors alone.

IX. SECURITY CAMERA SYSTEMS

A. Security camera systems installation designs must be approved by Campus Safety. Business use requirements for approved and required camera locations can be found in Section G403006, Surveillance Cameras of the University of Houston Campus Design Guidelines and Standards, Construction Systems and Assemblies.

B. All system installations must comply with UIT standards. Approved camera product lines and installation requirements can be found in the UH Network Infrastructure Standards, Section 12.

C. All installed systems shall use digital storage with approved archive durations and the ability to remotely monitor, control, and export video footage using a common interface. Wherever possible and where the facility involves multiple units, such installations shall be designed to provide immediate and future capacity for the entire facility. Any modifications to system components or model upgrades due to obsolescence must retain full compatibility with existing devices. Any exceptions to this policy must be approved by UIT and Campus Safety.

D. Autonomous stand-alone systems which do not comply with UH standards will not qualify for UHPD monitoring. Justifications for exceptions to this policy cannot be based upon cost factors alone.

X. SECURITY ALARM SYSTEMS

A. UIT will be responsible for maintaining an equipment standard to operate and manage the alarm monitoring services for the purpose of deterrence and/or detection of unlawful activity within facilities owned and/or operated by the University.

B. The system shall consist of a central host server, remote building control panels, and associated peripheral sensors and panic buttons. Communications between the central monitoring station and the remote panels shall be via the University data network.

C. Owners of electronic monitoring systems installed for administrative, maintenance or non-security purposes may optionally elect to participate in the central monitoring system. Examples would be devices for detection of gas buildup, or for flowing water or temperature monitoring in lab environments.

D. All such elective monitoring must be compatible with the central monitoring system and shall be subject to all provisions of this policy.

XI. RESPONSIBILITIES

A. Electronic Access Control

1. Building Coordinators (BCs), working in conjunction with the departments, are responsible to designate individuals to act as primary and secondary Department Access Users (DAUs). A minimum of two (2) DAUs, but no more than four (4) DAUs, must be assigned per building, dependent on the number of departments housed in the building.

a. BCs will work with Campus Safety in maintaining the buildings' access control and security systems program and public business hours designation.

b. Departments are responsible for controlling electronic Cougar Card access to building perimeter doors assigned to, or under the department's control and responsibility.

c. The department authorizing access for an individual is responsible for removing, verifying, or revoking access as required. This includes any metal keys or electronic access devices issued which allow access to department-controlled areas. All DAUs will need to develop a written procedure for removing, granting, approving, and reviewing user access. This written procedure should include the minimal standard for approving and granting access, as well as any additional departmental requirements.

The minimal standard for assigning access is as follows:

1) Cardholder has to have an active PeopleSoft status with UH.

2) Cardholder access has to be approved by the building/departments DAU for the area in which access was requested.

3) Access privileges are to be assigned with regards to the Security Zone to which access was assigned, which should include after-hours consideration.

4) All student badges must have a deactivation date at the time of access privileges being granted.

5) All access requests must be submitted using an Access Request Form, which will be audited once yearly by the Electronic Access Control Department.

d. Departments are responsible for all costs associated with installation of electronic access control on all interior doors. Departments are also responsible for all costs related to electronic access repair and replacement, upon the expiration of the one-year warranty provided by the Third Party Security Vendor.

NOTE: The exception is the interior doors installed as part of the original building construction project; these doors will be maintained by the Electronic Access Control department of Facilities/Construction Management; this exception excludes any abuse of neglect of the interior doors.

2. UIT is responsible for providing network connectivity to end appliances, managing the Level Application Database server, acquiring server software updates, and integrating other university systems.

3. Facilities/Construction Management (F/CM) is responsible for maintenance of access control panels, electrified hardware and low voltage wiring, wireless gateways, and card readers.

4. Campus Safety is the Access Control System Business Owner and is responsible for configuration management, acceptance testing, managing end users, training and escalation support, and the development of system policies and system management.

5. UHPD is responsible for providing after-hours access when warranted, and managing lock-down scenarios during critical events.

B. Camera System

1. UIT is responsible for the installation, maintenance and repair of cameras and recording devices, including network video recorders, Virtual Media (VM) application and database server hardware, and operating systems. UIT also performs physical calibrations when needed and provides testing facilities for proposed new devices to access systems compatibility and network impact. Additionally, UIT will provide Building Data Facilities for the installation of license plate processors.

2. F/CM is responsible for the physical infrastructure changes/modifications affecting prospective or existing systems to the installation of camera equipment.

3. Campus Safety is the Business Owner for the camera system and is responsible for initial system design and for securing design approvals from its customer, UHPD. Campus Safety manages end-user training and system-wide camera assessments for UHPD. Campus Safety also performs minor camera-NVR calibrations as needed.

4. UHPD is responsible for day-to-day operations, including systems monitoring, weekly testing of all cameras and Network Video Recorders (NVRs) to ensure their operational state, and for initiating repair work orders for failed devices. UHPD is also responsible for approving Campus Safety camera system designs for pre-installation, and project acceptance post-installation.

C. Alarm System

1. UIT is responsible for the installation and on-going maintenance of alarm systems.

2. F/CM provides infrastructure support as needed.

3. Campus Safety is the Business Owner of the Alarm System and is responsible for maintenance of the central receiving station and peripheral monitoring stations.

4. UHPD is responsible for monitoring alarm system status, and the site status for dispatching responding police officers.

D. Code Blue Phone System

1. F/CM is responsible for the physical infrastructure changes/modifications affecting prospective or existing systems.

2. UIT is responsible for the initial configuration of Code Blue devices, and for testing and maintaining the Voice Over Internet Protocol (VOIP) or analog telephone infrastructure.

3. Campus Safety is the Business Owner of Code Blue phones and is responsible for the system setup, testing, and maintenance of Code Blue devices.

4. UHPD manages the Code Blue communications.

E. For capital projects, fiscal responsibility for the installation, operation, and maintenance of electronic security systems shall be apportioned to the appropriate administrative units according to guidelines established by the Committee as approved by the Senior Vice President/Senior Vice Chancellor for Administration and Finance. All non-capital project installations will be funded by the requesting customer.

XII. POLICY REVIEW

The rapid pace of technological advances has the potential to significantly impact the provisions of this policy. Therefore, this policy shall be reviewed every three (3) years in order to ensure its relevancy.

XIII. REVIEW AND RESPONSIBILITY

Responsible Party: Assistant Vice President for Campus Safety

Review: Every three years on or before June 1

XIV. APPROVAL

Jim McShan

Senior Vice President for Administration and Finance

Renu Khator

President

Date of President's Approval: July 26, 2018

XV. REFERENCES

University of Houston Campus Design Guidelines and Standards, Section 08/28.13
- B2031 – Exterior Door Hardware
- C1025 – Interior Door Hardware
- C1030 – Access Controlled Egress Doors
- 28 13 00 – Electronic Access Control Specifications

UH Network Infrastructure Standards, Section 12

Building Coordinators Web Site

REVISION LOG

Revision Number	Approved Date	Description of Changes
1	03/23/2018	Initial version
2	07/26/2018	Required edits based on Internal Audit IT 2017-01 to Section XI.A.1.c. IT 2017-01 requires departments to develop written procedures for granting, approving, removing, periodically reviewing user access, reviewing public hours, and providing user awareness training