THE UNIVERSITY OF
TENNESSEE
KNOXVILLE

Knoxville Campus Procedure: SAAD002-K Physical Security	
Version 1	Effective Date: 04/23/2024

Objective

The University of Tennessee, Knoxville, ("UT" or the "University") is committed to enhancing the quality of life of the campus community by integrating technology with the safety and security best practices. A critical component of a comprehensive security plan is the utilization of electronic security equipment. Electronic security equipment is intended to help protect the safety and property of the UT community. This Campus Procedure on Physical Security (the "Procedure") is aligned with the university's core values.

This Procedure is adopted to formalize procedures for the installation and use of electronic security equipment and applies to all buildings owned or monitored by the University except residential halls and all UT employees, students, visitors, vendors, contractors, and others who use University buildings. Electronic security equipment is installed only after a determination that it is needed in accordance with this procedure.

Scope

Except for residential facilities, this procedure applies to all employees and units of UT in the use of electronic security equipment on the property owned or monitored by the University. All units using electronic security equipment are responsible for implementing and complying with this procedure in their respective operation. Note: All existing electronic security equipment in existence at adoption of this Procedure shall be maintained by units and will not be required to be replaced solely by adoption of this Procedure. However, any equipment that is replaced or added must adhere to the standards set forth herein. Unapproved or nonconforming electronic security equipment will be removed by UTPS Technicians.

A: **Access Control:** The physical control of buildings, offices, or other spaces on campus using one or more electronic security equipment. Examples: electronic locks, door contacts, motion alarms, glass break detectors, vault contacts.

B. **Life Safety:** Alarms utilized specifically to provide personal safety to persons on the campus. Examples: fire alarms, active threat barricade locks.

C. **Maintenance:** Alarms utilized to warn of environmental issues within campus facilities. Examples: Fire trouble alarms, electrical fault alarms, tamper alarms, controller alarms.

D. **Environmental:** Alarms utilized to warn of environmental issues within campus facilities. Examples: Water alarms, temperature alarms, path alarms for technical equipment.

E. **Panic:** Alarms utilized in extremely sensitive areas to provide a quick and discrete notification to the UT Police Unit of an emergency. Panic alarms are not recommended for most applications as they require at least a two Police Officer response and cannot be cancelled due to unintentional activation. Examples of common areas for panic alarms include locations that manage large sums of cash, narcotics (Pharmacy), or are routinely involved in the practice of employee or student disciplinary processes. Panic alarms require a site visit for approval from the Director of Physical Security, or designated personnel. No panic alarm shall be installed without this approval.

Roles

The Director of Physical Security (DPS), residing under the University of Tennessee Public Safety (UTPS), is responsible for implementation of this Procedure. The DPS has the authority to select, coordinate, operate, manage, and approve all campus electronic security equipment pursuant to this procedure. Specifically, the Central Alarm (CA) section of the Department of Physical Security oversees, monitors, and provides response to campus security alarms.

The Director of Physical Security shall monitor developments in the law and in security industry practices and technology to ensure that the university's use of electronic security equipment is consistent with the security industry's best practices and complies with all federal and state laws.

The Director of Physical Security will review unital proposals for electronic security equipment installations and review specific locations of electronic security equipment to determine that the application of these devices conforms to this procedure. Proposals for the installation of electronic security equipment shall be reviewed by UTPS prior to placement of equipment.

The Director of Physical Security will review any complaints regarding the utilization of electronic security equipment and determine whether this procedure is being followed. Appeals of a decision made by the Director will be made to and reviewed by the Associate Vice Chancellor of Public Safety.

DPS is responsible for advising units on appropriate applications of electronic security equipment and for providing technical assistance to units preparing proposals for the purchase and installation of electronic security and collaborating to provide appropriate access controls throughout the campus.

Definitions

Card Reader: an electronic device that recognizes an end user by id card or other known device to provide entry or for other designed function.

Card Reader with Electronically Controller Door: an electronic device that recognizes an end user by releasing upon proper credentials being presented.

Door Contact (Door Position Switches): a sensor that lets an alarm system know whether a door is open or closed.

Electrified Panic Hardware (Crash Bar): An electrically powered exit bar that releases upon proper access control programming or requested card access.

Electronic Security Equipment: Devices used to lock, unlock on a timer, deny, or approve access to sensitive areas, report movement within an area, report unusual or dangerous conditions such as fire, temperature or air hazards, dangerous behaviors, or other monitored conditions.

Electric Strike: An electrically powered mechanical lock or bolt that releases upon proper access control programming or requested card reader access.

Electronically Controlled Door: an electronically controlled door operating on a designated schedule used for public entrances during normal business hours.

Motion Sensor Alarm: a sensor that lets an alarm system know whether there is movement in a given area.

Pressure Sensor Alarm: a sensor that lets an alarm system know whether there is weight applied to a particular area.

Tamper Sensor Alarm: a sensor that lets an alarm system know whether a given object has been altered or meddled with.

Temperature Alarm: a sensor that lets an alarm system know whether the temperature has reached a predetermined temperature that is not ideal for a given area.

Unit: Any administrative, academic or research unit of the University of Tennessee, Knoxville.

Water Alarm: an alarm that lets an alarm system know it has detected water in an area where it should not be.

Procedure

I. General Principles

A. Control Standards and Placement of Security Equipment

The locations where security alarm equipment is installed may be restricted access sites such as a research lab or offices that provide financial transactions. Requests for utilizing electronic security equipment will be evaluated on a case-by-case basis by the Director of Physical Security.

Electronic security equipment may be installed in places where the security and safety of either persons or property, access control, or security of sensitive areas would be enhanced by the installation of such equipment. Electronic security equipment falls into several functional categories:

The installation of "dummy" electronic security equipment (i.e., equipment that does not operate) is prohibited. The Director of Physical Security will maintain an inventory of security alarm equipment installed pursuant to this procedure.

B. Access and Monitoring

Electronic security equipment is monitored 24 hours a day, 7 days a week. Security alarm equipment is monitored by UTPD Central Alarm staff as authorized by the Associate Vice Chancellor of Public Safety.

When an alarm is reported, UTPD officers (and/or appropriate unit) are sent to its location.

Central Alarm monitors only University electronic security system alarms. There are no private alarms monitored by Central Alarm.

C. Appropriate Use and Confidentiality

Electronic security records are considered confidential and can only be used for official university and law enforcement purposes upon the approval of the Associate Vice Chancellor of Public Safety or Director of Physical Security. Electronic security records shall be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure and in accordance with University of Tennessee System Policy IT0110 regarding Acceptable Use of Information Technology and the University of Tennessee System Policy IT0115 regarding Information and Computer System Classification.

II. Process

A. Installation

Units seeking approval for installation of electronic security equipment should obtain approval from the appropriate Dean, Vice Chancellor and/or unit head before requesting an estimate for installation and monitoring. In cases where the requesting unit is not in the same unit as the building owner, the requesting unit should also notify the building owner of the addition of the new alarms. The process for requesting alarm installation is through UT Facilities Management ARCHIBUS portal. If the requesting unit decides to proceed with alarm installation after reviewing the estimate, they should respond to the estimate agreeing to the terms (cost estimate and any applicable monitoring fees). The installation will be scheduled once the estimate has been approved by all parties. A list of building representatives can be found at https://fs.utk.edu/buildingrep/.

- Electronic security requests and installations must be received and approved by the Director of Physical Security prior to estimation and installation. This includes all access and alarm monitoring systems.

- Units will provide a request to the Director of Physical Security by email at physicalsecurity@utk.edu. A markup will be confirmed with the customer, and the Director of Physical Security will coordinate with Facilities Services regarding access control and alarm monitoring.

- Upon completion of the project, the alarm(s) will be added to the network by the installer upon DPS approved commissioning of all devices.

- Upon the project's completion, the customer will be provided with final information on any applicable annual costs and trained as applicable in the area where newly installed systems were applied.

The Director of Physical Security shall oversee the installation of all approved security alarm equipment.

Purpose of Panic Alarms with Basic description:

- For situations where you need help but cannot reveal to others that you are calling for help.
- Typically used by areas with cashiers or receptionists.
- Hidden for security reasons but should be accessible and known to immediate staff.
- Notifies alarm monitoring staff about an emergency or security breach.
- Alarm monitoring staff will send police to respond to location.
- Consists of panic buttons and the communication system that is used to send signals for needing emergency assistance.

UT Panic Alarms will consist of a single push button device located as requested. These devices will require the unit to fund the installation and pay installation costs along with an annual fee per device for monitoring and maintenance services.

Areas that can obtain a panic alarm must meet the following requirements:

1. Area is utilized on a consistent occupied and operational status.
2. Area has a high probability of volatile situations in an academic setting.

3. Area monitoring required for high value areas where personnel are present.

Panic Alarms are subject to review to ensure the security needs are relevant and being met.

Equipment Standard Specifications

The type of electronic security equipment and operating platform units shall use is equipment compatible with the campus-wide access control system. The Director of Physical Security maintains a list of approved alarm equipment for these purposes. Any approved equipment purchases exceeding $10,000 shall follow Fiscal Policy FI0410.

B. User and Administrative Responsibilities

UTPS Central Alarm operators shall be trained in the requirements of this Procedure and the technical, legal, and ethical parameters of appropriate electronic security equipment use. Training will be provided as needed by the Director of Physical Security or the manufacturer. CA will manage access controls except when Units have received approval to manage their own access controls.

Units seeking to manage their own access controls should submit a request by visiting the UT Physical Security website at https://safety.utk.edu/physical-security/. End users must obtain Unit Head level approval to be added to the system. Local controls may include the unital or building level authority to establish building lock/unlock schedules, and the ability to grant or remove access for internal users. UTPS employees will collaborate with these units to provide them with access controls for their assigned areas and provide training on managing controls (locking schedules, personnel access, etc.) within those areas.

Any misuse of the access control system noted by the DPS shall result in the revocation of privileges.

C. Access Request/Access Revocation (Timely Removal of Access)

Access Request (Employees)

To request electronic or mechanical/key access to a building or specific area, employees or sponsoring units shall visit the Access Management website at https://webapps.utk.edu/Facilities/AccessRequest2/

Student access is assigned automatically via integration with the university enrollment management system. However, if students require more access for employment or other educational needs, requests may be made through the Access Management website like employees. (Note: Residence Hall Access is not covered by this procedure and is managed solely by UT Housing.)

Access Revocation

Any access granted to the campus-wide access network is based on campus financial system (IRIS) cost center for the employee with access. Any changes to the employee's cost center status (retirement, resignation, termination or change in unit) will result in instant revocation of access privileges. If an employee changes cost centers, they will need to initiate a new access request.

Student access privileges are automatically revoked when the student's status changes. If a student drops a class, access for that class will be removed. Complete unenrollment, or completion of an academic term will result in the removal of all applicable access.

Access via UT VolCard ID card or approved smart device (Android/iPhone) is granted solely to the recipient. Campus users shall not permit others unknown to them to enter access-controlled buildings or doors with them (tailgate) or allow others to use their chosen device for building entry. Violations of this policy may result in loss of access privileges.

Emergency Access/Access Removal may be completed at any time by UTPD Central Alarm.

D. Services for Providing Operation and Assigning Access

Basic Service

Basic service includes Central Alarm programming of lock/unlock times of exterior doors on campus buildings.

- Also includes end user access to the Access Management website for access approvals and assignments referenced in section 3.3 of this Procedure.
- There is no fee for Basic Service.

Enhanced Services

Some units may have one or more internal access control areas (doors) that require specific programming and access permissions. These additional access control areas require additional programming beyond that of the "Basic Service" and will incur costs related to programming. Programming costs would include costs related to internal access scheduling. Further access would still be managed by the Access Request website referenced in section 3.3 of this procedure.

<u>Unit Managed Access Control</u>

Units approved to manage their own access (Section 3.2) will not incur additional costs for assigning access to their assigned areas unless they request additional services or support from Central Alarm.

E. **Fees for Alarm Installation and Monitoring**

Though misuse of access control devices will result in an "alarm" notification to Central Alarm, some Units may need more enhanced security given the sensitivity of their mission, equipment, or other such considerations. These Units may have need for motion alarms, panic alarms or other enhanced security equipment. Units making requests for this specialized equipment will be responsible for installation fees and monitoring fees, and the estimates for the fees will be approved prior to installation of electronic monitoring devices.

Charges related to installation and maintenance of alarms on campus are for cost-recovery.

Applicable monitoring fees are assessed annually and will increase with necessary adjustments for inflation, part costs, labor costs, and inventory modifications.

There will be no costs to individual units and/or other entities for physical security installations installed as part of the basic physical security best practices standards. This does not apply to most common areas and offices on campus.

Invoices related to installation and monitoring of electronic security utilize the following defined terms:

Access Zone: an electronically controlled door with or without a card reader that provides access via programming or card access.

Lockdown Switch: An electronic override switch that locks electronically controlled doors in an immediate emergency.

Panic Alarm: an alarm used to notify emergency services that help is needed.

Motion Alarm: a device that monitors activity in a particular area for unscheduled occupancy.

Remote Area Terminal (Alarm Keypad): a device that controls the alarm monitoring equipment in each area.

Door Contact (Door monitored for opening): a device that monitors door activity on a door for opening and closing.

Sensor (tamper, temperature, pressure): a device placed to monitor specific areas such as cabinets, area temperature, or pressure variance.

Priority response motion alarms (also called “burglar alarms”) and panic alarms are charged at an annual per device rate.

F. Procedure of the Use of Electronic Security Equipment

- Every user will be required to present their own credential on the appropriate electronic security identification card reader upon entry to any facility where required. Users will be able to use their UT issued VolCard and/or appropriately programmed mobile device (i.e., cell phone) where applicable.

- Vendor/Contractor access is assigned as needed upon request of a unit. Depending on the work being conducted by a vendor/contractor, certain unit approval may be needed, such as IT or Facilities.

- Panic buttons are to be used as intended for an emergency requiring immediate police response. Central Alarm performs periodic testing on these devices, coordinated through the unit possessing these alarms. Any activation of a panic alarm outside of Central Alarm scheduling is not permitted.

- All electronically controlled perimeter doors will be maintained by the Director of Physical Security as this provides ease and accessibility during business hours (scheduled openings of buildings). However, should Units decide to add additional door card readers or electronically controlled door(s) for the convenience of their faculty, staff, or students, that Unit shall be responsible for the cost of the devices and applicable installation fees.

- Schedules are determined by the building owner/representative.

  - If there are multiple Departments in a building each Department Head will coordinate with the building owner/representative to advise Central Alarm of the requested schedule.

- Any misuse and/or abuse of the access control system may result in revocation of administrative privileges of the access control system.

- Doors shall not be propped, held, or kept from closing by any means. If an employee believes a door needs to be completely open, then they must contact Central Alarm at 974-3114 prior to keeping the door open so police response will not be required.

- Panic Buttons are required to be tested quarterly by the assigned location.

Academic, Administrative, and Student Services Related Building Access:

Academic, administrative, and other instructional related buildings will be accessible to all University constituents during regularly scheduled academic instruction days and University scheduled workdays.

Access Management personnel shall consult with the Director of Physical Security about developing schedules for facilities and academic buildings requiring altered door schedules. Exterior door schedules are developed through coordination with building owners/representatives and Central Alarm personnel.

Central Alarm, with the Director of Physical Security, will accommodate after-hours and weekend academic class schedules except for those Units with localized controls.

Academic, administrative, and instructional-related building doors may allow access to secured perimeter exterior doors using an authorized UT ID card. After-hours access may be granted by utilizing an authorized UT ID card or smart device.

For locally managed units, building representatives may determine the hours and access granted to individuals utilizing card access. Units may consider the circumstances and instructional benefits for allowing access to individuals and students after hours.

Physical keys to any electronically controlled door may only be approved by the Director of Physical Security. Physical keys will not be issued without the express written consent of the Director of Physical Security.

Violations of this procedure include the following:

- Disabling automatic door closers, locking door hardware, or exit devices.
- Disabling any security or access device, including local exit alarms.
- Obstructing stairways, building exits, hallways, and doorways.
- Locking emergency exit doors in the path of free egress travel.
- Unauthorized use of barricade lock switches intended only for emergency situations.
- Unauthorized installation of locks, security equipment, or any other security devices.
- Unauthorized accumulation or duplication of keys or UT University ID cards.
- Unauthorized entry into mechanical, electrical, maintenance, or ITS closets.
- Sharing UT ID cards or keys.
- Using a UT ID card or key that is not your own or allowing others to use your UT ID card or key.
- Purposefully allowing others to follow you into a secured space without requiring them to use their UT ID
- Sharing UT ID PIN Codes.
- Using a PIN code that is not your own or allowing others to use your PIN code.
- Leaving exterior windows open and/or unsecured when room is unattended.
- Using keys on any electronically controlled doors with a card reader or otherwise electronically controlled.
- Propping open of any doors equipped with card access controls, automatically locking doors, normally locked doors, doors with local exit alarms, and any building exterior perimeter door.

G. Device Removal and Decommissioning

If a unit moves or otherwise decides they no longer need or want to utilize any alarm device, they must follow the installation procedures above and request a "decommissioning" of the devices. This notifies all parties involved that the devices should be removed from the system and no longer monitored. Fees related to alarm monitoring, maintenance, etc., will continue to be assessed to the Unit until the Unit requests decommissioning through the proper procedure. Billing will be stopped once a decommissioning request has been received.

Any decommissioned devices may be removed for repurposing of devices.

Units will be charged a decommissioning fee that will involve labor, patching, and general maintenance related items for removal, repurposing, or discarding requested devices.

If lock hardware needs to be replaced due to the decommissioning, the Unit must complete a work order with Facilities Services to have the appropriate mechanical door hardware installed.

There will be no removal of any devices without the express written consent of the Director of Physical Security or designee.

III. Physical Security Risk Assessment

The Director of Physical Security maintains a risk assessment of all campus buildings and establishes required minimum levels of access security based on risk tiers for each building. The DPS reviews this list and assigned risk tiers on an annual basis.

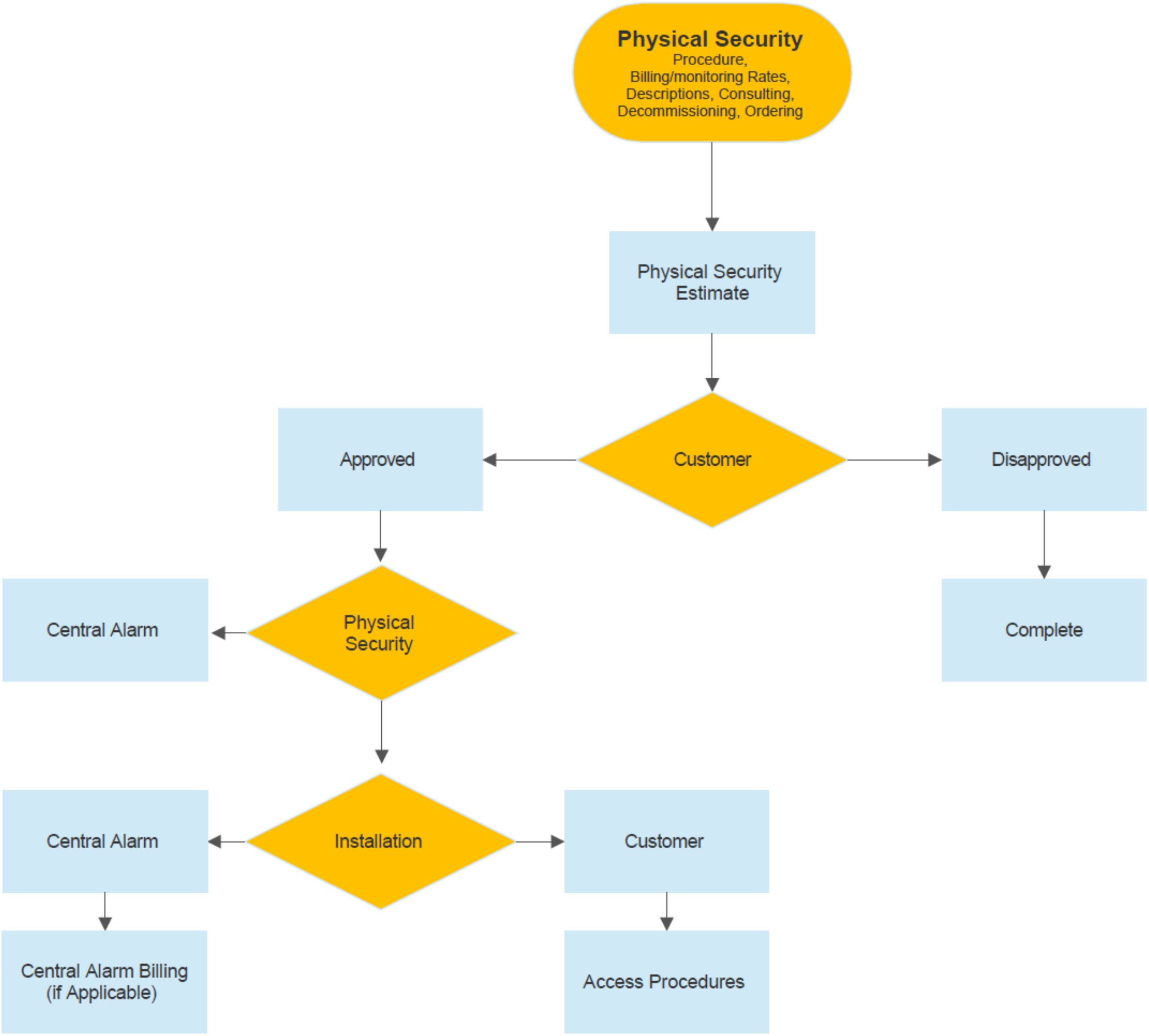
IV. Oversight & Management of Units Locally Managing Access

The DPS will maintain a documented process for oversight and management of departments that control their own access within the access management system, including training on access control expectations for users with elevated access rights.

V. Approval and Revisions

All revisions and approvals to this Procedure will be considered and finalized by the Chancellor's Cabinet as needed.

VI. Flow Chart


Physical Security
Procedure,
Billing/monitoring Rates,
Descriptions, Consulting,
Decommissioning, Ordering
Physical Security Estimate
Customer
Approved
Disapproved
Complete
Physical Security
Central Alarm
Installation
Central Alarm
Customer
Central Alarm Billing (if Applicable)
Access Procedures

Campus Responsible Official & Additional Contacts

This Campus Responsible Official and Additional Contacts section contains those who are responsible or share certain policy responsibilities, organized by subject matter, such as monitoring compliance with the policy, providing additional guidance on policy clarifications, organizing policy training, updating the policy, etc.

Subject Matter	Office Name	Telephone Number (xxx) xxx-xxxx	Email/Web Address
Policy Clarification and Interpretation	Public Safety	(865) 974-1000	physicalsecurity@utk.edu
Policy Training	Public Safety	(865) 974-1000	physicalsecurity@utk.edu