Section:	Information Security	Effective:	September 2005
Standard:	Physical Security for Electronic Information Resources	Revised:	
Policy Ref:	5.8.27	Responsibility:	Chief Information Security Officer

PHYSICAL SECURITY FOR ELECTRONIC INFORMATION RESOURCES STANDARD

Overview

The purpose of this standard is to explain the rules for granting, controlling, monitoring, and removing the different types of physical access used to protect the confidentiality, integrity, and availability of electronic information resources. It is intended to be complementary to the physical security requirements and guidelines of the University Police, and does not contradict or overrule those directives.

Scope

This Standard applies to all individuals within the UTHSCSA enterprise who use, own, manage, or support electronic information resources for the University.

Instructions

All electronic information resource devices shall be physically protected in direct proportion to the criticality and/or sensitivity of the information. A minimum level of physical security is required for all electronic information resources, and should increase in correlation to the classification of data (HOP Data Classification) stored on such devices.

At a minimum, physical security should include the following elements:

Administrative, Technical, and Physical Controls

- Administrative controls should exist to manage physical security of IT resources. These controls may include such things as procedures to follow in case of a fire or other emergency; who to contact in the event of a system shutdown or utility failures; employee maintenance activities; procedures for transfer and terminating employees; and procedures for periodic testing of physical equipment.
- Technical controls to manage physical security include such items as metal keys, badge access cards, entry logs, tokens, biometric devices, system locking programs; as well as software and devices that aid in the prevention of loss and the recovery of stolen or lost equipment.
- Physical controls are deployed to control, monitor, and manage access to a facility. These controls range from deterrents to detection mechanisms, and can be used to separate, isolate, and control access to various areas on a site. They may include motion detectors, sensors, alarms, fences, gates, lighting, and signs that clearly differentiate between public and restricted areas. UTHSCSA data and system owners with leased spaces should be aware of the access points to electronic information resources, including doors, windows, ceilings, and any other potential entrance into a facility.

Visitor Access

- All information resource facilities with sensitive information will log visitors and escort them while in the facility (HOP Data Classification).
- Visitors should be given the minimum access necessary to accomplish their function (Principle of Least Privilege).

Portable Devices

- Refer to Portable Computing Policy (HOP Portable Computing Policy)

Periodic Reviews

- The UTHSCSA data/system owner must conduct periodic reviews (minimum annually) of physical security measures for information resources. All information security incidents must be reported through normal incident reporting procedures (HOP Information Security Incident Reporting).
- The responsible person should review access rights for the information resource facility on a periodic basis and remove access for individuals no longer needing it. A list of people with access to the facility may be obtained from UT Police.

Physical Security Risks, Threats, Vulnerabilities, and Facility Location, Construction

- Information resource facilities can become the target of theft or malicious vandalism because of the equipment they contain, or the function the department performs. To help protect these locations, signage for server rooms and data processing facilities should be non-descript, so as to minimize unnecessary attention to the location.
- Workstations should be positioned to prevent unauthorized equipment access or viewing of information.
- Information resource facilities should be located in an area that minimizes exposure to physical hazards such as water, excessive heat or humidity, electrical power fluctuations, dust, or damage by storage and movement of other supplies.
- Backup media should be handled in a manner consistent with the Data Backup Policy (HOP Data Backup Policy).

Electrical Power Issues and Vulnerabilities

- Information resource facilities should provide sufficient backup power, power filtering, and surge protection to protect critical equipment and data; and to allow for safe shutdown within a reasonable time in case of power outages and brownouts.

Backup power may be used for an entire facility or applied to individual systems.

- If electronic information resources are located near electromagnetic interference (EMI) or radio frequency interference (RFI), then they should be shielded to prevent interference.

Fire Prevention, Detection, and Suppression

- Fire detectors, alarms, and suppression systems should be designed for the special conditions encountered in information resource facilities, as well as to comply with relevant building or fire codes.
- Appropriately rated portable fire suppression devices should be readily accessible, and personnel trained to use them.

Authenticating Individuals and Intrusion Detection

- The process for granting access to a secured facility must include approval by the data owner or their designees. Access approval shall be granted based on need, job responsibilities, and adequate background checks.
- The UTHSCSA data owner or their designees will remove the card and/or key access rights of individuals who have been terminated or who have transferred to job functions which do not require access to the secured facility.
- Issued secure access devices must not be shared, loaned, duplicated, or given to others; and must be returned to the data/system owner when they request or are no longer needed.