

## HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	December 2005
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.27</b>	<b>Physical Security for Electronic Information Resources</b>	Responsibility:	Chief Information Security Officer

# PHYSICAL SECURITY FOR ELECTRONIC INFORMATION RESOURCES

---

## Overview

The purpose of this policy is to establish the rules for granting, controlling, monitoring, and removing physical access in order to protect the confidentiality, integrity and availability of Health Science Center electronic information resources.

---

## Policy

This policy applies to all individuals who have access to Health Science Center, including UT Medicine, information resources. All electronic information resources shall be physically protected in relation to the criticality or sensitivity of the information. A minimum level of physical security is required for all electronic information resources. Security levels should increase in correlation to data classification, as described in the *Handbook of Operating Procedures* (HOP), [Section 5.8.21](#), "Data Classification" and should be reviewed at least on an annual basis.

At a minimum, physical security for information resources should include the following elements, which are expanded upon in the [Physical Security for Electronic Information Resources Standard](#). The [Physical Security for Electronic Information Resources Standard](#), as well as other security standards and guidelines pertaining to information security policies may be found at the Information Management and Services Web site <http://ims.uthscsa.edu/policies.aspx>.

- Administrative, technical, and physical controls
- Visitor access
- Portable devices
- Periodic reviews
- Facility location, construction, and vulnerabilities
- Physical security risks, threats, and vulnerabilities
- Electrical power issues and vulnerabilities

**HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES**

Chapter 5	Information Management & Services	Effective:	December 2005
Section 5.8	Information Security	Revised:	May 2011
<b>Policy 5.8.27</b>	<b>Physical Security for Electronic Information Resources</b>	Responsibility:	Chief Information Security Officer

- 
- Fire prevention, detection and suppression
  - Authenticating individuals and intrusion detection
- 

**Accountability**

Violations of this policy are subject to disciplinary action as described in the HOP, [Section 2.1.2](#), "*Handbook of Operating Procedures*".

---