5.8.27 Physical Security for Information Resources

Chapter 5 - Information Technology	Original Effective Date: December 2005
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised: October 2016

I. Purpose

To physically protect all Information Resources based on risk.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third-party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

All Information Resources must be physically protected based on risk.

A. Security controls must incorporate policies, standards and procedures for:

1. Protecting facilities in proportion to the criticality or importance of their function, the classification of data stored, transmitted or access by the Information Resource and the confidentiality of any Information Resources affected;
2. Managing access cards, badges, and/or keys;
3. Granting, changing and/or removing physical access to facilities to reflect changes in an individual's role or employment status; and
4. Controlling visitor and vendor physical access with procedures that incorporate the following:
    a. Advanced scheduling, logging and documenting of visits;
    b. Escorting while on premises; and
    c. Restricting the unauthorized use of photographic and video devices while on premises.

B. All Data Centers, Master/Main and Independent Distribution Facilities and Telecom Rooms must incorporate each of the following additional security controls:

1. Centrally managed access control system installed on all access points;
2. No externally facing windows;
3. Reviewing physical access semi-annually, or more often if warranted by risk;
4. Designating staff who will have authorized access during an emergency;
5. Monitoring the exterior and interior of the facility 24/7 by trained staff;
6. Maintaining appropriate environmental controls such as alarms that monitor heat and humidity, fire suppression and detection systems supported by an independent energy source and uninterruptable power systems capable of supporting all computing devices in the event of a primary power system failure; and
7. Electronic alarms for all entry points into the facility.

C. Accountability

Violations of this policy are subject to disciplinary action as described in the HOP, Section 2.1.2, "Handbook of Operating Procedures".

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

U.T. System (UTS) Policy

UTS 165 Information Resources Use and Security, Standard 16: Data Center Security

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
12/2005	Policy Origination		
10/2016	Policy Revision		
02/2023	Policy Review		