UTSA Institutional Compliance
Office of Information Security

OIS 28 – Standard for Physical Access

I. STANDARD STATEMENT

UTSA physical information resources must be protected in proportion to their criticality and confidentiality.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. All information technology facilities must have appropriate controls for granting and controlling access, monitoring the facility, and retracting permission for access when it is no longer needed. All individuals within the UTSA enterprise who are responsible for the installation and support of information resources, individuals charged with information resources security and data owners must follow these provisions, and the standard applies to multi-user and centralized computing facilities.

1. All multi-user computer and communications equipment must be located in locked rooms to prevent tampering and unauthorized use.
2. Physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
3. Access to information resource facilities must be granted only to the UTSA support personnel and contractors whose job responsibilities require access to that facility.
4. The process for granting card and/or key access to information resource facilities must include the approval of the manager of the facility.
5. Each individual who is granted access rights to an information resource facility must receive training in emergency procedures for that facility and must sign the appropriate access and non-disclosure agreements.
6. Access cards and/or keys must not be shared by or loaned to others.

7. All information resource facilities that allow access to visitors will track that access with a sign in/out log.
8. Card access records and visitor logs for mission-critical information resource facilities must be kept for routine review, based on the criticality of the resources being protected.
9. Visitors must be escorted while in access-controlled areas of information resource facilities.
10. The manager of the information resource facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
11. The manager of the information resource facility must review card and/or key access rights for the facility on a periodic basis and remove access for individuals who no longer require access.
12. All information storage media (such as hard disk drives, flash drives and CD-ROMs) containing sensitive information must be physically secured when not in use.

Title: OIS 28 – Standard for Physical Access
Effective Date: December 1, 2010
Last Revised: August 4, 2020