**Texas A&M University-San Antonio**

**29.01.03.O0.09  Physical Access**

Approved: June 16, 2014
Next Scheduled Review: June, 2019

---

**Procedure Statement**

Technical support staff, security administrators, system administrators and others, may have physical facility access to information resource as part of their job responsibilities. The granting, controlling and monitoring of the physical access to information resources facilities is extremely important for overall security and protection of University assets.

---

**Reason for Procedure**

This purpose of this Procedure is to establish the rules for granting, controlling, monitoring and removal of physical access to facilities that contain information resources. The purpose of the implementation of this Procedure is to provide a set of measures that will mitigate information security risks associated with physical access. There may also be other or additional measures that ITS, department heads, or deans will provide to further mitigate risks. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this Procedure based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

---

**Official Responsibilities and Procedure**

1. All facilities supporting information resources must be physically protected in proportion to the criticality and confidentiality of their function and the information contained with the physical location.

2. The process for granting card and physical key access to information resources facilities must include the approval of the IRM.

3. The department that issues the access card or physical key (i.e. facilities, ID Card Office, UPD, or CIO) will be responsible for maintaining proper documentation. Access to
facilities or locations that contain information resources must be approved by the Information Resource Manager (IRM).

4. Access to Information Resources facilities must be granted only to Texas A&M University-San Antonio (A&M-San Antonio) support personnel and contractors, whose job responsibilities require access to that facility.

5. Access cards and physical keys must not be shared with others.

6. Visitors must be escorted by staff personnel with clearance in card access controlled areas of information resources facilities.

7. All physical security systems must comply with applicable regulations, including but not limited to, building codes and fire prevention codes.

8. Signage for restricted access rooms and locations must be practical. Minimal discernible evidence of the importance of the location should be displayed.

9. Access cards and physical keys that are no longer required must be immediately returned to the issuing office by the employee (i.e. facilities, ID Card Office, UPD, or CIO). Cards must not be reallocated to another individual bypassing the return process. As part of the termination process, it is the supervisor’s responsibility to ensure that all access cards and physical keys are returned.

10. Lost or stolen access cards and physical keys must be immediately reported to the issuing department (i.e. facilities, ID Card Office, UPD, or CIO) and Information Security Officer (ISO) or Information Resource Manager (IRM).

11. Physical access records shall be maintained as appropriate for the criticality of the Information Resources being protected. Such records shall be reviewed as needed by the Information Resources Manager (IRM).

Non-Compliance

Violation of this Procedure may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of the employment relationship in the case of contractors or consultants; dismissal for interns and volunteers; or in the case of students suspension or expulsion administered based on the Code of Student Conduct. Additionally, individuals are subject to loss of access and privileges to the University information resources, civil, and/or criminal prosecution.
Related Rules

DIR Practices for Protecting Information Resources Assets

Family Educational Rights and Privacy Act (FERPA)

Gramm Leach Bliley Act (GLB Act)

Health Insurance Portability and Accountability Act (HIPAA)

TAMU System Policy 29.01 Information Resources

Texas Administrative Code (TAC) 202 as amended or supplemented

Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education

Definitions

Accounts - Information resource users are typically assigned access to an information resource using logon credentials, which include, at the minimum, a unique user name and password.

Confidential Information - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

Custodian - Guardian or caretaker (the holder of data). The agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

Information Resources (IR) - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

Information Resources Manager (IRM) - The Information Resources Manager (IRM) oversees the acquisition and use of information technology within a state agency or university. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and comply with regulations and agency policies.
**Information Security Officer (ISO)** - Responsible to the executive management for administering the information security functions within the agency. The ISO is the internal and external point of contact for all information security matters.

**Information Technology Services (ITS)** – The designated name for the central information technology department for the University.

**Mission Critical Information** - Information that is defined by A&M-San Antonio or information resource owner to be essential to the continued performance of the mission of A&M-San Antonio or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of A&M-San Antonio or department.

**Owner** - The manager or agent responsible for the function which is supported by the resource; the individual upon whom responsibility rests for carrying out the appropriate use and safeguards for the resource. Where appropriate, ownership may be shared by managers of different departments.

**System Custodian** – Guardian or caretaker of the operating system and physical hardware; the person(s) charged with implementing the controls specified by the owner of the system. This custodian is responsible for operating system updates and assisting the Application Custodian with any testing or major changes to the system.

---

**Contact Office**

Finance and Administration, Information Technology Services (210)784-4357 (HELP)