Texas A&M University System Standard – Physical Access

Standard Statement

The purpose of the System Office (SO) physical access standard is to establish the process for the granting, control, monitoring, and removal of physical access to information resource facilities.

Definitions

Confidential Information - Information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act. Refer to the System Regulation 29.01.03 and the related Data Classification Standard for more 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.

Mission Critical Information - information that is defined by the SO or information resource owner to be essential to the continued performance of the mission of the SO and its departments. 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, and failure to comply with regulations or legal obligations, or closure of the department.

Information Resource Owner - an entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Responsibility and Standards

1. GENERAL

   Technical support staff, system administrators, and others may have information resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to information resource facilities is extremely important to an overall security program. The purpose of the SO physical access standard is to establish the process for the granting, control, monitoring, and removal of physical access to information resource facilities.

2. APPLICABILITY

This standard applies to facilities that house multi-user systems (i.e., "data centers") that process or store mission critical and/or confidential information.

The information resource owner, or designee, is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with standard *Exclusions from Required Risk Mitigation Measures*.

Responsibility for ensuring secure physical access to information resources may be part of the job function for departmental staff which may include, but not be limited to, information technology staff, system administrators, supervisors, managers, and others.

3. STANDARDS

3.1 All physical security systems shall comply with applicable regulations, such as, but not limited to, building codes and fire prevention codes.

3.2 Physical access procedures to all information resources facilities shall be documented and managed.

3.3 All information resource facilities shall be physically protected in proportion to the criticality or importance of their function at the SO.

3.4 Access to information resources facilities shall be granted only to appropriate SO personnel, vendors, or other authorized personnel whose job responsibilities require access to that facility.

3.5 There shall be an approval and documentation process for granting and revocation/return of security codes, access cards, and/or key access to information resources facilities.

3.6 Individuals who are granted access rights to an information resource facility must sign appropriate access agreements. Facilities users should also receive information regarding appropriate physical security practices and emergency procedures.

3.7 Security access codes, access cards and/or keys to information resource facilities shall not be shared or loaned to others.

3.8 Appropriate departmental personnel responsible for the physical security of information resources shall review access rights for the facility on a periodic basis and revoke access for individuals that no longer require such access.

3.8.1 Access cards or keys must not be reallocated to another individual bypassing the return process.

3.8.2 Access cards and/or keys must not have identifying information other than a return mail address.

3.9 Visitors must be escorted in restricted access areas of information resource facilities.

3.10 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 organizational unit heads or their designees.

3.11 Signage for restricted access rooms and locations must be practical, yet display minimal discernible evidence of the importance of the facility.

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Officer.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer