The Division of Information Technology
University Information Security Standards

Information Security Standard – Physical Access (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

Information Technology support staff, system administrators, and information security administrators may have information resource physical facility access requirements as part of their job duties. The granting, controlling, and monitoring of the physical access to information resource facilities is enormously important to an overall security program.

2. Applicability

This procedure applies to facilities that house multi-user systems that process or store mission critical and/or confidential information. The purpose of the implementation of this information security standard 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 department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures is to be determined by the department heads and their identified information security administrators. 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 is 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).

The intended audience includes, but is not limited to, all information resources data/owners, management personnel, system administrators, and other university personnel with required access to IT facilities.

3. Definitions

3.1 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.

3.2 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook

computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.3 Information Resources Manager (IRM): Responsible to the State of Texas for management of the agency/university's information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the agency. If an agency does not designate an IRM, the title defaults to the agency's Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

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

4. Procedures

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

4.2 Physical access to all information resources restricted facilities must be documented and managed.

4.3 All information resources facilities must be physically protected in proportion to the criticality or importance of their function at West Texas A&M University.

4.4 Access to information resources facilities must be granted only to West Texas A&M University support personnel and contractors, whose job responsibilities require access to that facility.

4.5 The process for granting card and/or key access to information resources facilities must include the approval of the chief information officer (CIO)/information resources manager (IRM) for West Texas A&M University.

4.6 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.

4.9 Access cards and/or keys must not be shared or loaned to others. Piggybacking or allowing others to enter the building using your access card is not permitted.

4.10 Access cards and/or keys that are no longer required must be immediately returned to the appropriate person (i.e. university lock shop manager, CIO/IRM). Cards must not be reallocated to another individual bypassing the return process.

4.11 Lost or stolen access cards and/or keys must be immediately reported to the chief information officer (CIO)/information resources manager (IRM) for West Texas A&M University.

4.12 Cards and/or keys must not have identifying information other than a return mail address.

4.12 Visitors must be escorted in card access controlled areas of information resources facilities.

4.12 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) for West Texas A&M University or their designees.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer