Information Technology Services
Physical Access Standard

Approved: February 11, 2020

Standard Statement

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.

Reason for Standard

The purpose of the Tarleton State University physical access standard is to establish the process for the granting, control, monitoring, and removal of physical access to information resource facilities and, in addition, provide a set of measures that will mitigate information security risks associated with physical access. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee. 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 standard based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer. This standard applies to facilities that house multi-user systems (i.e., "data centers") that process or store mission critical and/or confidential information. Responsibility for ensuring secure physical access to information resources may be part of the job function for departmental staff that may include, but not be limited to, information technology staff, system administrators, supervisors, managers, and others.

Standards and Responsibilities

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

2. Physical access standards to all information resources facilities shall be documented and managed.

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

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

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.

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.

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

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.
   - Access cards or keys must not be reallocated to another individual, bypassing the return process.
   - Access cards and/or keys must not have identifying information other than a return mail address.

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

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.

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.

Information Resources (IR): the standards 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 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, failure to comply with regulations or legal obligations, or closure of a department or the university.

Contact Office

Information Technology Services
CIO of Information Technology Services
254.968.9395