TEXAS A&M INTERNATIONAL UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.14 Physical Access

First Approved: March 28, 2013
Revised: June 22, 2017
Next Scheduled Review: June 22, 2022

Procedure Statement and Reason for Procedure

Technical support staff, security administrators, system administrators, and others may have Information Resource physical facility access requirements as part of their duties. The granting, controlling, and monitoring of the physical access to Information Resources facilities is extremely important for an overall security program.

The purpose of this SAP is to establish the process for granting, controlling, monitoring, and removing physical access to Information Resource facilities. It applies to individuals within Texas A&M International University (TAMIU) who are responsible for the installation and support of Information Resources, individuals charged with Information Resources security, and data owners. This SAP supplements *TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities* and *TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources*.

Procedures and Responsibilities

1. Physical Access

    1.1 All Information Resources must be physically protected based on risk in accordance with associated risk management decisions as part of the overall TAMIU security program.

1.2 Physical access safeguards help to establish best practices for the appropriate granting, controlling, and monitoring of physical access for all facilities supporting Information Resources. Physical access safeguards include the following:

1.2.1 All facilities supporting Information Resources must have physical access controls in proportion to the importance, sensitivity, and accountability requirements of the data and systems housed in that facility.

1.2.2 Access to facilities supporting Information Resources will only be granted to authorized personnel of TAMIU and other contractors or personnel whose job responsibilities require such action.

1.2.3 Access/ID cards and/or keys must not be shared with others. Access/ID cards and/or keys that are no longer required must be returned to the Office of Human Resources. Cards must not be reallocated to another individual.

1.2.4 Lost or stolen access/ID cards and/or keys will have access removed and must be reported to the responsible department contact, the University Police Department, and the Office of Information Technology (OIT) as soon as possible.

1.2.5 Access and log records for facilities supporting Information Resources are the responsibility of the department that manages the facility. Requests for access must come from the applicable TAMIU data/system owner.

1.2.6 The department in charge of facilities supporting Information Resources must be notified within 3 business days if individuals who had access to those facilities should no longer have access due to a change in roles, completion of contract, or other reason that negates their need for further access.

1.2.7 Visitors must be escorted in controlled areas of facilities supporting Information Resources.

1.2.8 The department in charge of facilities supporting Information Resources must review access records periodically and investigate any unusual access.

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

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

1.2.11 The process for granting card and/or key access to Information Resources facilities must include the approval of the person responsible for the facility.

1.2.12 All Information Resources facilities that allow access to visitors will track visitor access with a sign in/out log based upon the criticality of the Information Resources.

1.2.13 Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.

1.2.14 The person responsible for the Information Resources facility must remove the ID card and/or key access rights of individuals who change roles within TAMIU or are separated from their relationship with TAMIU.

Related Statutes, Policies, Regulations, or Rules

Texas Administrative Code 202, Subchapter C – Information Security Standards for Institutions of Higher Education
TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources
TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities

Appendix

References:
Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
The State of Texas Information Act
Texas Government Code, Section 441
Texas Administrative Code, Chapter 202
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Contact Office

Office of Information Technology, 956-326-2310