TEXAS A&M INTERNATIONAL UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.37 Clean Desk

First Approved: March 28, 2013
Revised: January 31, 2019
Next Scheduled Review: January 31, 2024

Procedure Statement and Reason for Procedure

In order to protect sensitive information, it is essential to follow specific guidelines. The purpose of this SAP is to outline specific measures that ensure an environment that reduces security threats and risks. This SAP:

- establishes procedures to reduce security threats,
- emphasizes the importance of protecting physical office documents from malicious parties, and
- establishes procedures to reduce risks for physical information security incidents.

This SAP applies equally to all Texas A&M International University (TAMIU) employees and on-campus third party contractors who work with TAMIU sensitive information.

Procedures and Responsibilities

---

1. Procedures

   All TAMIU employees and on-campus third party contractors who handle TAMIU information must adhere to the following practices to ensure protection from unauthorized access, alteration, exposure, or destruction.

   1.1 Based on the level of risk, confidential and sensitive documents should be stored inside locked drawers when employees are away from their desks for extended periods of time (e.g., lunch breaks).

1.2 At the end of each working day, employees should clear their workstations of all office documents that contain confidential or sensitive materials and should ensure that desks and filing cabinets are locked.

1.3 Portable computing devices (i.e., laptops, tablets, etc.) and mass storage devices (i.e., CD's, DVD's, USB drives) must be secured in locked cabinets or drawers or similar protections to protect against theft.

1.4 Whenever possible, TAMIU employees should scan confidential and sensitive documents and file them electronically in secure systems (i.e., Laserfiche, encrypted hard drive). Refer to TAMIU SAP 29.01.99.L1.24, *Encryption*.

1.5 Confidential and sensitive documents that are no longer required should be properly destroyed (i.e., shredding). This includes duplicates of forms with such data.

Related Statutes, Policies, Regulations, or Rules

TAC 1, Part 10, Chapter 202, Subchapter C – Information Security Standards for Institutions of Higher Education

TAMIU Rule 29.01.99.L1, *Information Resources*

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, itsecurity@tamiu.edu