TEXAS A&M INTERNATIONAL UNIVERSITY

Standard Administrative Procedure (SAP)

29.01.99.L1.10 Intrusion Detection

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

Procedure Statement and Reason for Procedure

The Texas A&M International University (TAMIU) network infrastructure is provided as a central utility for all users of TAMIU Information Resources. Intrusion detection plays an important role in implementing and enforcing an organizational security policy. As Information Resources grow in complexity, effective security systems must evolve. When dealing with distributed systems there are multiple vulnerability points that trigger and necessitate assurance that networks and systems are secure. Intrusion detection aims to provide this assurance.

The purpose of this SAP is to establish procedures for the access and use of the network infrastructure. These procedures are necessary to preserve the integrity, availability, and confidentiality of TAMIU Information Resources. This SAP applies to all individuals with access to TAMIU Information Resources.

Procedures and Responsibilities

1. Procedures and Responsibilities

   At TAMIU, several systems are used to monitor, detect, and log intrusion attempts via the network. Invariably, these intrusion detection systems provide the Information Security Officer (ISO) with invaluable access to logs that monitor, measure, and detect anomalies. If an event occurs in which the network infrastructure is threatened, appropriate measures will be taken in accordance with the Incident Response Plan. Anomalous activity detected in audit logs and reports will be reported in accordance with procedures outlined in TAMIU SAP 29.01.99.L1.08, *Incident Management*.

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