29.01.99.K1.090 Intrusion Detection Standard Administrative Procedure

Effective: April 1, 2004
Revised: April 25, 2013
Revised: March 13, 2019
Next Scheduled Review: March 13, 2024

Introduction

Intrusion detection plays an important role in implementing and enforcing an institutional security program at Texas A&M University-Kingsville (TAMUK). Intrusion detection systems are a part of a layered defense for identification of threats from external sources. Intrusion detection provides early warning of potential internet and network based threats.

Purpose

The purpose of this procedure is to establish the rules for intrusion detection.

Audience

This procedure applies to system administrators, individuals charged with information resource security, data owners, and individuals who are responsible for information resource security.

Intrusion Detection Procedure

1. Operating system, user accounting, and application software logging processes must be enabled on server systems and network appliances.
   a. The system administrator will furnish any audit logs as requested by the Information Security Officer (ISO) or Security Analyst.
2. Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
3. Audit logging of any firewalls and other network perimeter access control system must be enabled.
4. Audit logs from the perimeter access control systems must be reviewed by Network Services.

5. Controlled penetration test of perimeter security must be performed on an annual basis.
6. Any suspected intrusions must be reported to the ISO.

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of students. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References

1. DIR Practices for Protecting Information Resources Assets
2. The State of Texas Information Act
3. Texas Administrative Code, Chapter 202
4. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
5. System Regulation 29.01.03 Electronic Information Services Access and Security

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404