Intrusion Detection Procedure

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 provide the first line of 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 individuals that are responsible for the installation of new information resources, the operations of existing information resources, and individuals charged with information resources security at TAMUK.

Intrusion Detection Procedure
1. Operating system, user accounting, and application software audit 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 employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References
1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441