Procedure Statement

The Texas A&M University-San Antonio (A&M-San Antonio) network infrastructure is provided as a central utility for all users of University 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. Intrusion detection systems can provide part of this assurance.

Reason for Procedure

This A&M-San Antonio applies to all users of A&M-San Antonio information resources.

The purpose of the implementation of this Procedure is to establish the rules for intrusion detection. These rules are necessary to preserve the integrity, availability and confidentiality of A&M-San Antonio’s information resources.

This Procedure applies to all individuals with access to A&M-San Antonio information resources.

Official Responsibilities and Procedure

1. The University operates systems that are used to monitor, detect and log intrusion attempts via the IP network. These systems include intrusion detection systems, firewalls, email virus scanning, antivirus protection for servers and workstations. Anomalies will be investigated and appropriate measures will be taken in the event of an actual threat in accordance with 29.01.03.O0.08 Incident Management.

2. All suspected and/or confirmed instances of host, server, or network intrusions will be reported immediately as outlined in 29.01.03.O0.08 Incident Management to the Information Security Officer (ISO).
3. Operating system, user accounting and application software audit processes will be enabled on all host and server systems where resources permit.

4. Alarm and alert functions, as well as audit logging of any firewalls and other network perimeter access control systems will be enabled.

5. Logs from the firewalls and network perimeter access control systems will be monitored and reviewed as risk management decisions warrant.

6. Logs for servers and devices will be monitored and reviewed as risk management decisions warrant.

7. The ISO will work with the CIO/IRM to remediate any identified risk or intrusions to the A&M-San Antonio network.

---

**Non-Compliance**

Violation of this Procedure may result in disciplinary action, which may include termination of employment for full-time and part-time employees; a termination of the employment relationship in the case of contractors or consultants; dismissal of interns and volunteers; or in the case of students suspension or expulsion administered based on the Code of Student Conduct. Additionally, individuals are subject to loss of access and privileges to the University information resources, civil, and/or criminal prosecution.

---

**Related Statutes, Policies, or Requirements**

- DIR Practices for Protecting Information Resources Assets
- Family Educational Rights and Privacy Act (FERPA)
- Gramm Leach Bliley Act (GLB Act)
- Health Insurance Portability and Accountability Act (HIPAA)
- Texas Administrative Code (TAC) 202 as amended or supplemented
- Texas Administrative Code (TAC) 202.75 Security Standards for Institutions of Higher Education
- TAMU System Policy 29.01 Information Resources
- TAMU System Regulation 29.01.03 Electronic Information Services Access and Security
A&M-San Antonio Procedure 29.01.03.O0.08 Incident Management

**Definitions**

**Accounts** - Information resource users are typically assigned access to an information resource using logon credentials, which include, at the minimum, a unique user name and password.

**Confidential Information** - Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

**Custodian** - Guardian or caretaker (the holder of data). The agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information.

**Incident Report** – A formal reporting of a known information technology related incident. This is performed by completing the associated ITS form.

**Information Resources (IR)** - The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

**Information Resources Manager (IRM)** - The Information Resources Manager (IRM) oversees the acquisition and use of information technology within a state agency or university. The IRM ensures that all information resources are acquired appropriately, implemented effectively, and comply with regulations and agency policies.

**Information Security Officer (ISO)** - Responsible to the executive management for administering the information security functions within the agency. The ISO is the internal and external point of contact for all information security matters.

**Information Technology Services (ITS)** – The designated name for the central Information Technology department for the University.

**Mission Critical Information** - Information that is defined by A&M-San Antonio or information resource owner to be essential to the continued performance of the mission of A&M-San Antonio or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of A&M-San Antonio or department.
**Network Scanning** - The process of transmitting data through a network to elicit responses in order to determine configuration state or the presence of security vulnerabilities within an information system.

**Owner** - The manager or agent responsible for the function which is supported by the resource; the individual upon whom responsibility rests for carrying out the appropriate use and safeguards for the resource. Where appropriate, ownership may be shared by managers of different departments.

**Security Incident** - Assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing, disruption or denial of service, altered or destroyed input, processing, storage, or output of information, or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

**Security Incident Reporting System (SIRS)** - The electronic system used for reporting (after the fact, after-action) incidents in compliance with Texas Department of Information Resources (DIR) regulations.

**System Custodian** – Guardian or caretaker of the operating system and physical hardware; the person(s) charged with implementing the controls specified by the owner of the system. This custodian is responsible for operating system updates and assisting the Application Custodian with any testing or major changes to the system.

**User** - An individual or automated application or process that is authorized to the resource by the owner, in accordance with the owner’s rules and procedures.

**Vulnerability** - A weakness or flaw in system security design, implementation, procedures or controls that can cause a violation of the system’s security policy or a security breach if exploited by an attacker.

---

**Contact Office**

Finance and Administration, Information Technology Services (210) 784-4357 (HELP)