Procedure Statement

The Texas A&M University-San Antonio (A&M-San Antonio) network infrastructure is provided as a central utility for all users. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high-speed networking technology to allow the future provision of enhanced user services.

Reason for Procedure

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

The purpose of this Procedure is to establish the rules for the maintenance, expansion and use of the network infrastructure. This Procedure is necessary to preserve the integrity, availability and confidentiality of A&M-San Antonio information resources. This Procedure applies to all individuals with access to A&M-San Antonio information resources.

Official Responsibilities and Procedure

1. Information Technology Services (ITS) is responsible for A&M-San Antonio networking infrastructure which includes all cabling, wireless signaling and connected electronic devices to ensure reliability of operations, proper accessibility to resources, and protection of data integrity.

2. All hardware connected to an A&M-San Antonio supported or operated network is subject to ITS management and monitoring standards.

3. ITS is responsible for ensuring the following are duties are performed in support of A&M-San Antonio network configuration:
3.1 A&M-San Antonio network infrastructure configurations;

3.2 The management of any changes, adds, and enhancements to the University network;

3.3 Operating and maintaining a reliable network with appropriate redundancy requirement to meet quality of service goals;

3.4 Installing or authorizing a third-party vendor to install all cabling and network hardware;

3.5 Maintaining a list of network inventory connected to the A&M-San Antonio network;

3.6 Authorizing changes to the configuration of active network management devices.

3.7 Ensuring A&M-San Antonio firewalls are installed and configured following 29.01.03.O0.10 Firewall Management.

4. Users must not extend or re-transmit network services in any way. Network aggregation devices (i.e. router, switch, hub, wireless access point) must not be connected without ITS approval.

5. The use of departmental firewalls is not permitted without the written authorization from the A&M-San Antonio IRM.

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 for 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 Rules

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

A&M-San Antonio Procedure 29.01.03.O0.10 Firewall Management

A&M-San Antonio Procedure 29.01.03.O0.17 Network Access

A&M-San Antonio Procedure 29.01.03.O0.38 Vendor Access

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.

**Logon ID** - A unique account name that is required as the first step in logging into a secure information resource. A logon ID typically must be associated with a user password to obtain access to the information resource.

**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.

**Production System** - The hardware, software, physical, procedural and organizational issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.

**Scheduled Change** – A system modification accompanied by a formal notification received, reviewed, and approved by the review process in advance of the change being made.

**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.

**Security Patch** - A fix or repair to a program that eliminates a known system vulnerability.
**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.

**Unscheduled Change** – A system modification that fails to present notification to the formal process in advance of the change being made.

**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)