Procedure Statement

The network infrastructure is provided by Texas A&M University-San Antonio (A&M-San Antonio) for all authorized users. It is important that network infrastructure, which includes media, active electronic equipment (i.e., routers, switches, cables, etc.) and supporting software, be able to meet current business performance requirements.

Reason for Procedure

This Procedure applies to all University network information resources.

The purpose of this Procedure is to provide a set of measures that will mitigate information security risks associated with network access. There may also be other or additional measures that department heads or deans will provide to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and the identified information security administrators. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this Procedure based on documented information security risk management decisions and business functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO) or the Information Resources Manager (IRM).

The University Network Access Procedure applies equally to all individuals with access using any University or Non-University owned information resource.

Official Responsibilities and Procedure

1. Management of network addresses, address space, and network naming will be managed by Information Technology Services (ITS). ITS is required to approve all access methods, installation of all network hardware, and requirements for attaching any computer system or device to the A&M-San Antonio operated network. This process ensures that access to the network does not interfere with the operation and reliability of the network.
2. Users shall notify ITS when any network connected information resources have been transferred, replaced, or decommissioned.

3. Users are not permitted to extend or re-transmit network wired or wireless services in any way. Any network aggregation devices (e.g. hubs, switches, routers) shall be approved by the University Information Security Officer (ISO) or the Information Resources Manager (IRM) before being connected to the network infrastructure.

4. Anonymous access to the network is not permitted.

5. Network management or other monitoring devices shall not be connected to network infrastructure without approval by the ITS department.

6. End-users shall not connect or install any information resource device that is not provided and supported by the University without approval by ITS. Additionally, end-users shall not alter or disable University network infrastructure devices or equipment.

7. Virus protection software must not be disabled or bypassed except as required by the temporary installation of software or for other authorized special circumstances.

8. Remote access to the University network is only authorized through approved and supported means (e.g. SSL VPN, VPN client, etc.) provided by ITS.

9. Remote access by contractors or vendors must be approved by the IRM and follow the procedure set forth in 29.01.03.O0.26 Vendor Access.

10. Non-University computers or devices connecting to the network provided by the University must conform to all appropriate security standards for information resources.

11. ITS reserves the right to inspect any system or equipment connecting to the network and disconnect as necessary for business or other risk related reasons.

---

**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.O0.01 Electronic Information Services Access and Security**

**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.

**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.

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

**Contact Office**

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