Procedure Statement

Network scanning is frequently used to generate a network security report detailing possible vulnerabilities of the systems attached. The operating systems and applications for all information resource must undergo a regular vulnerability assessment in accordance with Texas Administrative Code 202 - Information Security Standard.

Reason for Procedure

This Procedure applies to all users of Texas A&M University-San Antonio (A&M-San Antonio) information resources.

The purpose of the implementation of this Procedure is to gather information that will be used for network scanning and vulnerability assessment, including notifying owners of vulnerabilities, determining incorrectly configured systems, validating firewall access requests, and gathering network census data.

Official Responsibilities and Procedure

1. Information Technology Services (ITS) will conduct network scans and network vulnerability scans of devices attached to the University network.

2. Network scans or network vulnerability scans must be authorized by IRM or designee.

3. Under no circumstances may network scanning be conducted by unauthorized users.

4. Owners of information resources found to be vulnerable will be contacted by the Information Security Officer (ISO) concerning the identified risk(s). The information resource owner is responsible for ensuring that the identified risk(s) is mitigated in a timely manner.
5. A vulnerability assessment will be conducted by DIR at least annually.

6. Other exceptions to these guidelines may be authorized only by the A&M-San Antonio President, IRM, or designee.

---

**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**

---

**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.

**Internet** - A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies and colleges.

**Intranet** - A private network for communications and sharing of information similar to the Internet, but accessible only to authorized users within an organization. An organization’s intranet is usually protected from external access by a firewall.

**ISACC (Information Security Awareness Assessment and Compliance)** - A web-based system used to assess the security posture of information systems and measure compliance with the Information Security Standards.

**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.

**Malicious code** – Software code that infects information resource and allows them to operate in a manner that is inconsistent with the intentions of the user and which typically results in annoyance or damage to the user’s information systems. Examples of such software include:

- **Viruses** - Pieces of code that attach to host programs and propagate when an infected program is executed.
- **Worms** - Particular to networked computers to carry out pre-programmed attacks that jump across the network.
• Trojan Horses - Hide malicious code inside a host program that appears to do something useful.
• Attack scripts - These may be written in common languages such as Java or ActiveX to exploit weaknesses in programs; usually intended to cross network platforms.
• Spyware - Software planted on your system to capture and reveal information to someone outside your system. It can do such things as capture keystrokes while typing passwords, read and track e-mail, record the sites visited, pass along credit card numbers, and so on. It can be planted by Trojan horses or viruses, installed as part of freeware or shareware programs that are downloaded and executed, installed by an employer to track computer usage, or even planted by advertising agencies to assist in feeding you targeted ads.

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.

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.

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)