**Procedure Statement**

Wireless networks provide a network connection that can be used without any physical connection within a limited area (e.g. building). Wireless networking is not intended to replace a wired connection. This Procedure is a supplement to the Network Access Security.

**Reason for Procedure**

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

The purpose is to establish the procedures for the access and use of the wireless network. These procedures are necessary to preserve the integrity, availability and confidentiality of A&M-San Antonio information resources.

**Official Responsibilities and Procedure**

1. Wireless networking is available by connecting to the applicable A&M-San Antonio SSID, opening a browser, and navigating to [http://www.tamus amt.us.edu](http://www.tamusamt.us.edu) if you are not automatically redirected there. Valid credentials are required in order to sign on and receive wireless access.

2. Wireless access must be password protected and access must be linked to an individual through authentication mechanisms.

3. If confidential and/or sensitive information is accessed through the wireless network, then that information must be encrypted as defined in 29.01.03.O0.13 *Encryption of Confidential and Sensitive Information*. 
4. Information resources security controls must not be bypassed or disabled unless reviewed and approved by the Information Resources Manager (IRM) or delegated Information Security Officer (ISO).

5. Information Technology Services (ITS) will monitor for unauthorized wireless access points. Any unauthorized access point detected on the A&M-San Antonio network will be disconnected from the network and a security incident will be filed by the ISO per procedure 29.01.03.O0.08 Incident Management.

6. Only approved wireless clients are allowed to access the A&M-San Antonio wireless network.

7. The manufacturer default settings of the Service Set Identifier (SSID) must be changed upon initial configuration of any wireless access device. All default passwords must also be disabled or changed.

______________________________

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.O0.08 Incident Management

A&M-San Antonio Procedure 29.01.03.O0.13 Encryption of Confidential and Sensitive Information

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).

**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.

**Logon ID** - A unique account name that is required as the first step in logging into a secure information resource. Generally, 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 Procedure or information resource owner to be essential to the continued performance of the mission of A&M-
San Antonio Procedure 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 Procedure or department.

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

**SSID** - Service Set Identifier is the name of a wireless local area network (LAN). All wireless devices on a wireless LAN must employ the same SSID in order to communicate with each other.

**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.

---

**Contact Office**

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