The Division of Information Technology
University Information Security Standards

Information Security Standard – Wireless Access (Legacy TAC 202)
Approved: April 15, 2005
Last Revised: July 26, 2017
Next Scheduled Review: August 2018

1. General

Wireless networking using IEEE 802.11 is a powerful but immature technology that may pose security risks and management problems. The main objective of the wireless network is to provide a network connection that can be used virtually anywhere within limited areas (e.g., a lecture room or meeting room); it is not intended to be a replacement for the wired infrastructure. Before planning the installation of any wireless LAN equipment, contact Network Services through the Information Technology Service Center. The procedures provided herein are necessary to preserve the integrity, availability, and confidentiality of West Texas A&M University information when utilizing wireless connectivity to access West Texas A&M University information resources.

2. Applicability

The West Texas A&M University Wireless Access information security standard applies equally to all groups and individuals that utilize wireless connectivity to access West Texas A&M University information resources. This includes students, faculty, and staff members as well as guest account users. This information security standard also applies to all wireless network devices accessing or connected to the university network infrastructure.

The purpose of the implementation of this information security standard is to provide a set of measures that will mitigate information security risks associated with the use of wireless network technology on the campus of WTAMU.

The intended audience includes any University employee, student, guest, or visitor that uses the wireless network at WTAMU.

3. Definitions

3.1 Confidential Information: information that is excepted from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act. Examples of "Confidential" data may include, but are not limited to:

(1) Personally identifiable information such as a name in combination with social security number (SSN) and/or financial account numbers

(2) Student education records

(3) Intellectual Property such as copyrights, patents, and trade secrets

(4) Medical records

3.2 Information Resources: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3.3 Mission Critical Information: information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University 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 the University or department.

3.4 Owner of an Information Resource: an entity responsible:

(1) for a business function (Department Head); and,

(2) for determining controls and access to information resources

3.5 Sensitive Personal Information: an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted

(1) Social security number

(2) Driver's license number or government-issued identification number or
(3) Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

3.6 IEEE 802.11: The family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 committee, which establishes standards for wireless Ethernet networks. 802.11 standards define the over-the-air interface between wireless clients and a base station or access point that is physically connected to the wired network.

3.7 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.

3.8 Wireless Access: A type of local area network (LAN) that uses high-frequency radio waves rather than wires to communicate between nodes. A wireless LAN spans a relatively small area using on or more of the following technologies to access information resources systems:

(1) Wireless local area network – based on the IEEE 802.11 family of standards.

(2) Wireless personal area network – based on the Bluetooth and/or infrared (IR) technologies.

(3) Wireless handheld devices – includes text-messaging devices, personal digital assistants (PDA's) and smart phones.

3.9 Information Security Officer (ISO): Responsible to the executive management for administering the information security function within the agency. The ISO is the university's internal and external point of contact for all information security matters.

4. Procedures

4.1 Requests for wireless service must be architected, engineered, provided, and maintained by Network Services at all times. Vendors and/or external service providers are not authorized to engineer network or wireless services without the explicit approval of network services or the IRM.

4.2 Requests for wireless service within any departmental networks must be approved by Network Services and or the IRM. No departmental wireless coverage is permitted outside of West Texas A&M buildings.

4.3 Network Services will install and maintain all wireless access points, to ensure they meet minimum security requirements (i.e. changing of SSID).

4.4 Requests for wireless service for stand-alone networks must also be approved by Network Services.

4.5 The attachment of unapproved wireless access points, bridges, and/or repeaters is strictly prohibited at West Texas A&M University. This also includes the residential living network.

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

4.7 Network Services will monitor for unauthorized wireless access points. Any such rogue access point detected on the West Texas A&M University network shall be disconnected from the network and a security incident will be filed with the information security officer (ISO).

4.8 Confidential information, mission critical or sensitive personal information shall not be accessed by wireless communication unless the communication is at least encrypted by strong encryption as determined by the information security officer (ISO).

4.9 Information resource security controls must not be bypassed or disabled.

4.10 The manufacturer default settings of the Service Set Identifier (SSID) shall be changed upon initial configuration of any wireless access device.

OFFICE OF RESPONSIBILITY: Information Technology

CONTACT: Chief Information Officer