Texas A&M University System Standard – Wireless Access

Standard Statement

The standards provided herein are necessary to preserve the integrity, availability, and confidentiality of System Office (SO) information when utilizing wireless connectivity to access SO information resources.

Definitions

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.

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:

- Social security number;
- Driver's license number or government-issued identification number; or
- 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.

Confidential Information - sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act) and other constitutional, statutory, judicial, and legal agreements. Refer to the System Regulation 29.01.03 and the related data classification standard for more information.

Examples of “Confidential” data may include but are not limited to:

- Personally Identifiable Information (PII), such as: a name in combination with Social Security number (SSN) and/or financial account numbers
- Student Education Records
- Intellectual Property, such as: Copyrights, Patents and Trade Secrets
- Medical records

Mission Critical Information - information that is defined by the System Office or information resource owner to be essential to the continued performance of the mission of the SO. 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, and failure to comply with regulations or legal obligations, or closure of the department.

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.

Wireless Access – access to a type of non-physical network that uses high-frequency radio waves rather than wires to communicate between end points. A wireless network spans a relatively small area using one or more of the following technologies to access the information resources systems:

- Wireless Local Area Networks--Based on the wireless networking standards.
- Wireless Personal Area Networks--Based on the Bluetooth and/or Infrared (IR) technologies.
- Wireless Handheld Devices--Includes text-messaging devices, Personal Digital Assistant (PDAs), and smart phones.

Owner of an Information Resource - An entity responsible for:

- A business function; and,
- Determining controls and access to information resources supporting that business function.

Official Standards

1. General

Wireless networking using wireless technologies 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 dining area); it is not intended to be a replacement for the wired infrastructure. Before planning the installation of any wireless LAN equipment, contact TAMU Network and Information Security Group (NIS) or the Security Operations Center (SOC).

The following steps are necessary to preserve the integrity, availability, and confidentiality of SO information.

2. Applicability

The System Office wireless access standard applies equally to all groups and individuals that utilize wireless connectivity to access System Office information resources. This includes students, faculty, and staff members as well as guest account users.

The information resource owner or designee (e.g., custodian, user), is responsible for ensuring that the risk mitigation measures described in this standard are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures provided in this standard. All exclusions must be in accordance with the standard *Exclusions from Required Risk Mitigation Measures*.

3. Standards

3.1 Wireless networking is available in most System Office buildings through Tamulink. Detailed information about Tamulink can found at http://tamulink.tamu.edu/.

3.2 Requests for wireless service in NIS-maintained building networks must be engineered and provided by NIS.

3.3 Requests for wireless service within SO networks, i.e. those not maintained by NIS, must be approved by NIS.

3.4 No wireless coverage is allowed outside SO buildings. Overlap between wireless nodes will be arbitrated by NIS.

3.5 SO wireless information resource managers and users must insure that Service Set Identifiers (SSID) values are changed from the manufacturer default setting for wireless local area networks (LAN). Some networks should not include organizational or location information in the SSID.

3.6 Wireless access must be password protected.

3.7 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 System Chief Information Security Officer.

3.8 Non-System Office computer systems that require wireless network connectivity must conform to TAMU NIS standards and must be approved in writing by the TAMU NIS department.

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

3.10 Unattended devices utilized for wireless access must be physically secure allowing only authorized physical access.

Related Statutes, Policies, or Requirements

Supplements System Regulation 29.01.03

Contact Office

For interpretation or clarification, contact The Texas A&M University System Chief Information Officer.

OFFICE OF RESPONSIBILITY: The Texas A&M University System Chief Information Officer