

STANDARD ADMINISTRATIVE PROCEDURES

29.01.99.M1.30 Information Resources – Wireless Access

Approved June 10, 2009

Next Scheduled Review: June 17, 2012

Standard Administrative Procedure Statement

The procedures provided herein are necessary to preserve the integrity, availability, and confidentiality of TAMU information when utilizing wireless connectivity to access TAMU 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.

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

- Personally Identifiable Information, 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

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.

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.

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 - a type of [local-area network](#) (LAN) that uses high-frequency radio waves rather than wires to communicate between [nodes](#). A Wireless LAN [computer 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 IEEE 802.11 family of 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 Procedures

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 dining area); it is not intended to be a replacement for the wired infrastructure. Before planning the

installation of any wireless LAN equipment, email the Network and Information Security Group (NIS) at consult@net.tamu.edu.

The following procedures are necessary to preserve the integrity, availability, and confidentiality of TAMU information.

2. Applicability

The TAMU Wireless Access Standard Administrative Procedure applies equally to all groups and individuals that utilize wireless connectivity to access TAMU 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 SAP 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 SAP. All exclusions must be in accordance with SAP 24.99.99.M1.27 Exclusions from Required Risk Mitigation Measures.

3. Procedures

- 3.1 Wireless networking is available on the Texas A&M University (TAMU) campus through Tamulink. Detailed information about Tamulink can be 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 departmental networks, i.e. those not maintained by NIS, must be approved by NIS. No departmental wireless coverage is allowed outside TAMU buildings.
- 3.4 Requests for wireless service for stand-alone networks, i.e. those that do not access TAMU systems or the internet, must be approved by NIS. Send requests to consult@net.tamu.edu.
- 3.5 Unapproved attachment of wireless access points is strictly prohibited in TAMU residence halls.
- 3.6 No wireless coverage is allowed outside TAMU buildings. Overlap between wireless nodes will be arbitrated by NIS. Proposals or information regarding stand-alone wireless networks should be sent via

email to consult@net.tamu.edu.

- 3.7 TAMU 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.
- 3.8 Wireless access must be password protected.
- 3.9 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 Chief Information Security Officer.
- 3.10 Non-TAMU computer systems that require wireless network connectivity must conform to TAMU NIS standards and must be approved in writing by the TAMU NIS department. Call the CIS help desk for assistance (845-3800) or send an email request to consult@net.tamu.edu
- 3.11 Information resource security controls must not be bypassed or disabled.
- 3.12 Unattended devices utilized for wireless access must be physically secure allowing only authorized physical access.

Related Statutes, Policies, or Requirements

Supplements [University Rule 29.01.99.M1](#)

Contact Office

For interpretation or clarification, contact [Information Technology Issues Management](#).

OFFICE OF RESPONSIBILITY: [Associate Provost of Information Technology](#)