PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.28 Information Resources – Wireless Access

Approved March 28, 2013
Revised June 11, 2018
Next Scheduled Review: June 2023

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to preserve the integrity, availability and confidentiality of Prairie View A&M University (PVAMU) information when utilizing wireless connectivity to access PVAMU 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.

Confidential Information - information that is confidential pursuant to state or federal law. Such information may also be subject to state or federal breach notification requirements. See the Texas A&M University System Data Classification Standard for additional information.

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.

Service Set Identifier (SSID) - 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 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; and,
- Wireless Handheld Devices - Includes text-messaging devices, Personal Digital Assistant (PDAs), and smart phones.

Information Resource Owner - an entity responsible for a business function and for determining controls and access to information resources supporting that business function.

Official Procedures and Responsibilities

---

1. GENERAL

1.1 Wireless networking using IEEE 802.11 is a powerful 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, the following procedures are necessary to preserve the integrity, availability and confidentiality of PVAMU information.

2. APPLICABILITY

2.1 This UAP applies equally to all groups and individuals that utilize wireless connectivity to access PVAMU 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 UAP 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 UAP. All exclusions must be approved in writing by the Information Security Officer (ISO).

3. PROCEDURES

3.1 Wireless networking is available on all PVAMU campuses.

3.2 All wireless service is provided by Information Technology Services (ITS).

3.3 Requests for wireless service for stand-alone networks, i.e. those that do not access PVAMU systems or the internet, must be submitted in writing and approved by the ISO and ITS Department.

3.4 Unauthorized attachment of wireless access points is strictly prohibited in all PVAMU buildings.

3.5 Wireless access must be password protected; and, all users must be authenticated before connecting to the PVAMU wireless network.

3.6 Confidential information and mission critical information shall not be accessed by public wireless communication unless the communication is at least encrypted by strong encryption as determined by the ISO (such as approved PVAMU VPN access).

3.7 Information resource security controls must not be bypassed or disabled by anyone who utilizes wireless connectivity to access PVAMU information resources.

Related Statutes, Policies, Regulations and Rules

Tex. Admin. Code Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education

Security Control Standards Catalog

System Policy 29.01 Information Resources

System Regulation 29.01.03 Information Security

Contact Office

Office of Information Resources Management	936-261-9350