

**PRAIRIE VIEW A&M UNIVERSITY
ADMINISTRATIVE PROCEDURES**

29.01.03.P0.07 Information Resources – Network/Wireless Access

Approved (May 26, 2009)

Next Scheduled Review (May-2012)

1. PURPOSE

- 1.1 The information resources network infrastructure is provided by Prairie View A&M University for all University departments. It is important that the infrastructure, which includes media, active electronic equipment (i.e., routers, switches, cables, etc.) and supporting software, be able to meet current performance requirements, while retaining the flexibility to allow emerging developments in high-speed networking technology and enhanced user services.

Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources. Prairie View A&M University has developed rules and procedures that address acceptable use of information resources. The purpose of this University Administrative Procedure (UAP) is to identify those relevant policies and procedures.

This UAP applies to all University information resources.

- 1.2 The purpose of the implementation of this SAP is to provide a set of measures that will mitigate information security risks associated with acceptable use of University information resources. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures will be determined by the information resource owner or their designee. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this SAP based on information security risk management decisions and business functions. Such risk management decisions must be documented and reported to the designated Information Security Officer.
- 1.3 The intended audience for this SAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of University information resources.

2. DEFINITIONS

- 2.1 Anonymous write capability - the ability of people to save (on Prairie View A&M University computers) information they create without their identity being known (to system administrators).
- 2.2 Anonymously originating network traffic - causing a (Prairie View A&M University) computer system to send traffic via the network where the custodian/owner is not known.

- 2.3 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.

3. PROCEDURES AND RESPONSIBILITIES

- 3.1 Network management/control devices shall not be connected to network infrastructure without prior consultation with the Information Technology Services department.
- 3.2 Management of network addresses and name space is managed by Information Technology Services. Users are permitted to use only those network addresses issued to them by Network Services Group of Information Technology Services.
- 3.3 End-users are not to connect to or install any equipment to the network infrastructure without prior approval from Information Technology Services. Additionally, end-users shall not alter or disable University network infrastructure devices or equipment.
- 3.4 Network scans and network vulnerability scans of devices attached to the Prairie View A&M University network as well as the appropriate remediation are occasionally necessary to ensure the integrity of Prairie View A&M University computing systems. Network scans and network vulnerability scans may only be conducted by University employees designated by the organizational unit head responsible for the information resource.
- 3.5 Individuals controlling right-to-use for systems attached to the network infrastructure will ensure only authorized persons are granted access.
- 3.6 Allowing anonymous write capability to University systems or anonymously originating network traffic requires Information Resources permission.
- 3.7 Users shall not alter University-owned network hardware in any way.
- 3.8 [Airspace Guidelines](#) for Using the 2.4 and 5.0 GHz Radio Frequency.
- 3.9 Link to: [AirspacePolicy3.doc](#) for complete guidelines.

Contact Office: Information Security Officer; 936-261-2126