UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to establish the process for change of the network infrastructure. In addition, the performance of these procedures is necessary to ensure compliance with the Texas Administrative Code 202.75 Information Resources Security Safeguards.

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.

Information Security Officer (ISO) - person responsible to the executive management for administering the information security function within the University. The ISO is the University’s internal and external point of contact for all information security matters.

Official Procedures and Responsibilities

1. GENERAL

1.1 The information resources network infrastructure is provided by Prairie View A&M University (PVAMU) 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.

1.2 There may be additional measures that department heads or deans will implement to further mitigate risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the department heads and their identified information security administrators. In accordance with Texas Administrative Code 202.75 Information Resources Security Safeguards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this UAP based on documented information security risk management decisions and business
functions. Such risk management decisions must be documented and approved by the designated Information Security Officer (ISO).

2. **APPLICABILITY**

2.1 This UAP applies to all University network infrastructure information resources. The intended audience for this UAP includes, but is not limited to, all information resources management personnel, owners, system administrators, and users of University information resources.

3. **PROCEDURES AND APPROVAL PROCESS**

3.1 All network connected equipment must be configured to a specification approved by PVAMU Information Technology Services.

3.2 All hardware connected to the PVAMU network is subject to its Information Technology Services management and monitoring standards.

3.3 Changes to the configurations of active network management devices must not be made without the approval of Information Technology Services.

3.4 The University network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by the Information Technology Services.

3.5 All connections of the network infrastructure to external third party networks are the responsibility of PVAMU Information Technology Services. This includes connections to external telephone networks.

3.6 The use of departmental firewalls is not permitted without the written authorization from Information Technology Services.

3.7 Users must not extend or re-transmit network services in any way. Devices such as routers, switches, hubs, or wireless access points cannot be installed on the PVAMU network without approval from Information Technology Services.

3.8 Users must not install network hardware or software that provides network services without PVAMU Information Technology Services approval.

3.9 Users are not permitted to alter network hardware in any way.

---

**Related Statutes, Policies, Regulations and Rules**

- **System Policy 29.01 Information Resources**
- **System Regulation 29.01.03 Electronic Information Services Access and Security**
- **Texas Administrative Code 202.75 Information Security Standards**