UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to establish the process for user access to the University’s 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

Anonymous Write Capability - the ability for people to save information they have created on a computer system without their identity being known to system administrators.

Anonymous Proxies - tools that attempt to make activity on the Internet untraceable.

Backhaul - transmitting data beyond its normal destination point and back again to utilize network equipment not available at the destination location. It is typically used to mask the location of the point of origin.

Anonymously Originating Network Traffic - the ability to cause a computer system to send traffic via the network for which the custodian/owner is not known.

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.

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 PVAMU network 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

3.1 Network management/control devices shall not be connected to the network infrastructure without prior consultation with the Office of Information Technology Services (ITS).

3.2 Management of network addresses and name space is managed by ITS. Users are permitted to use only those network addresses issued to them by the Network Services Group of ITS.

3.3 End-users are not to connect to or install any equipment to the network infrastructure without prior approval from ITS. 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 PVAMU network as well as the appropriate remediation are occasionally necessary to ensure the integrity of PVAMU 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 privileges for systems attached to the University 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.

Related Statutes, Policies, Regulations and Rules