PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

29.01.03.P0.07 Information Resources – Network Access
Approved May 26, 2009
Revised November 4, 2014
Revised August 14, 2017
Reviewed December 22, 2022
Next Scheduled Review: December 1, 2027

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

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.

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 Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education, 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 Center for Information Technology Excellence.

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

3.3 End-users are not to connect to or install any equipment to the network infrastructure without prior approval from the Center for Information Technology Excellence. 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 or authorized third-party vendors designated by the ISO or Chief Information Officer. In addition, the Security Operations Center (SOC), part of the Texas A&M University System, will monitor and scan the network and attached devices and stores for security purposes.

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 Users shall not alter university-owned network hardware in any way.

Related Statutes, Policies, Regulations and Rules

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

System Policy 29.01 Information Resources

System Regulation 29.01.03 Information Security

The Texas A&M University System Information Security Standards

Security Control Standards Catalog

Contact Office	
Center for Information Technology Excellence	936-261-9350