

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



29.01.03.P0.06 Information Resources – Network Configuration

Approved May 26, 2009
Revised November 4, 2014
Revised August 14, 2017
Revised January 19, 2023
Next Scheduled Review: January 1, 2028

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 [Ch. 202, Subch. C, Information Security Standards for Institutions of Higher Education](#).

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 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 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 equipment must be configured to a specification approved by PVAMU Center for Information Technology Excellence (C.I.T.E).
- 3.2 All hardware connected to the PVAMU network is subject to its Information Technology Services management and monitoring standards, including the Security Operations Center (SOC), per System Regulation [29.01.03 Information Security](#), Section 2 System Security Operations Center Authority and Responsibility.
- 3.3 Changes to the configurations of active network management devices must not be made without the approval of the C.I.T.E.
- 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 C.I.T.E.
- 3.5 All connections of the network infrastructure to external third-party networks are the responsibility of the C.I.T.E. This includes connections to external telephone networks.
- 3.6 The use of departmental firewalls is not permitted without the written authorization from the C.I.T.E.
- 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 the C.I.T.E.
- 3.8 Users must not install network hardware or software that provides network services without approval from the C.I.T.E.
- 3.9 Users are not permitted to alter 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
