PRAIRIE VIEW A&M UNIVERSITY

UNIVERSITY RULE

21.01.06. P1  Security of Electronic Information Resources
Date Approved: (June 02, 2009)

Rule Statement

The Prairie View A&M University’s electronic information resources are vital academic and administrative assets and require appropriate safeguards. Computer systems, networks, and data are vulnerable to a variety of threats. These threats may compromise the integrity, availability, and confidentiality of the information. Effective security programs shall be employed to appropriately eliminate or mitigate the risks posed by potential threats to the University’s information resources. Requirements, procedures, and responsibilities for applying the standards described in our University Administrative Procedures to protect these resources against unauthorized access, disclosure, modification or destruction whether accidental or deliberate are described below.

Reason for Rule

Prairie View A&M University, as a State University, is required to comply with the Texas Administrative Code (TAC) on “Information Security Standards”. The TAC assigns responsibility for protection of informational resources to the President. For the purposes of this rule, the authority and responsibility regarding the University’s compliance with the Texas Administrative Code on information Security Standards has been delegated by the President to the Vice President for Business Affairs and the Prairie View Chief Information Officer.

Procedures and Responsibilities

1. Responsibilities

1.1 The Vice President for Business Affairs has designated the Information Security Compliance Officer and Chief Information Officer as the entities responsible for administering the provisions of this rule and the TAC Information Security Standards. The procedures for administering the TAC Standards are included in University Administrative Procedures 21.01.06.P1.01-.19.

1.2 The head or director of a department shall be responsible for ensuring that an appropriate security program is in effect and that compliance with this rule and TAC Standards is maintained for information systems owned and operated by the department.

1.3 The head or director of a department which provides operational support (custodian) for information systems owned by another PVAMU department shall have the responsibility for ensuring that an appropriate security program is in effect and that compliance with TAC Standards is maintained for the supported information systems.
1.4 Operational responsibility for compliance with TAC Standards may be delegated by the department head or director to the appropriate information system support personnel (e.g. System Administrators) within the department.

1.5 Mission Critical or Confidential Information maintained on an individual workstation or personal computer must be afforded the appropriate safeguards stated in the TAC Standards. It is the responsibility of the operator, or owner, and/or departmental Systems Administrator of that workstation or personal computer to insure that adequate security measures are in place.

2.0 Compliance Assessment Reporting

2.1 Departments having ownership or custodial responsibility for electronic information systems ensure that on an annual basis, a security assessment report is filed with the Office of the Vice President. This report is produced by the ISSAC system. The report shall be filed by the designated system administrator or custodian of the information system.

2.2 Departments having responsibility for information resources which store, transmit, or process mission critical or confidential information must access their security posture and measure their compliance with the TAC Information Security Standards by using the Information Security Awareness Assessment and Compliance ISSAC system.

Related Statutes, Policies, or Requirements

3.0 Definitions

3.1 Confidential Information – Information that is exempt from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal laws. Most student records are confidential records.

3.2 Mission Critical Information – Information that is defined by Prairie View A&M University or any division thereof (department, etc.), to be essential to their function(s) and would cause severe detrimental impact if the data/system were lost and unable to be restored in a timely fashion.

3.3 Owner – A person responsible for a University function and for determining controls and access to electronic information resources supporting that University function.
3.4 Custodian – A person (or department) providing operational support for an information system and having responsibility for implementing owner-identified controls and access privileges.

3.5 ISSAC – (Information Security Awareness Assessment and Compliance) – A web-based system used to assess the security posture of information systems and measure compliance with the Information Security Standards. It also provides guides for creating a disaster recovery plan and performing a physical security check. Additionally, a security training course (information and test) is provided.

Related Statutes, Policies or Requirements

Texas Administrative Code, Title 1, Chapter 202

TAMUS Regulation 21.01.06

Contact Information

Vice President for Business Affairs
936-261-2150

System Approvals

Approved for Legal Sufficiency:

[Signature]
Andrew L. Strong
General Counsel

[Signature]
Michael D. McKinney
Chancellor

5/28/09
Date

6/2/09
Date