

**24.99.99.W1/PR Security of Electronic Information Resources**  
*Approved March 8, 2005*

**1. GENERAL**

West Texas A&M University (WTAMU) electronic information resources are vital academic, research and administrative assets, which require appropriate safeguards. Computer systems, networks, and data are vulnerable to a variety of threats. These threats have the potential to compromise the integrity, availability, and confidentiality of the information.

Effective security programs must be implemented to appropriately eliminate or mitigate the risks posed by potential threats to WTAMU electronic information resources. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction whether accidental or deliberate, as well as to ensure the availability, integrity, utility, authenticity and confidentiality of information. Access to state electronic information resources must be appropriately managed.

WTAMU, as a state institution of higher education, is required to comply with the Texas Administrative Code (TAC) on "Information Security Standards." The Texas Administrative Code assigns responsibility for protection of informational resources to the University President. For the purposes of this rule, the authority and responsibility regarding University compliance with the Texas Administrative Code (TAC) on Information Security Standards has been delegated by the president to the chief information officer.

**2. DEFINITIONS**

- 2.1 Confidential Information - Information that is excepted 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.
- 2.2 Mission Critical Information - Information that is defined by Texas 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.
- 2.3 Owner - A person responsible for a University function and for determining controls and access to electronic information resources supporting that University function.
- 2.4 Custodian - A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges.

- 2.5 ISAAC (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.

### **3. CONTROLS AND RESPONSIBILITIES**

- 3.1 The chief information officer has designated the director of systems support/assistant to the CIO, who is the appointed information security officer for the University, as the individual responsible for administering the provisions of this rule and the TAC Information Security Standards.
- 3.2 The information security officer shall ensure that on at least an annual basis, a University-wide electronic information resources security risk management plan and disaster recovery plan are sent to the Office of Chief Information Officer. WTAMU divisions and departments having ownership or custodial responsibility for electronic information systems shall ensure that on at least an annual basis, a division/department electronic information resources security risk management plan and a disaster recovery plan are sent to the Office of Chief Information Officer. The division/department head or designated custodian of the information system(s) shall file the required reports.
- 3.3 For systems that are not centrally managed by the Division of Information Technology, the management of access to WTAMU electronic information resources is delegated to division/department heads or equivalent. The processes or procedures to be used by division/department heads or equivalent should include establishing security standards, computer accounts, granting physical access and removal and/or deletion of access in accordance with WTAMU Information Resources Security Standard Administrative Procedures that deal with: Account Management, Administrator/Special Access Management, Password/Authentication, Vendor Access, and Physical Access.
- 3.4 The information security officer is responsible for implementing electronic backups as a business requirement to enable the recovery of data and applications for systems that are centrally managed by the Division of Information Technology. He/she shall ensure that security monitoring procedures, up-to-date virus protection software and intrusion detection systems are in place. Division/department heads or their equivalents are responsible for implementing electronic backups, security monitoring procedures, the use of intrusion detection systems where resources permit, and up-to-date virus protection software for systems that are not centrally managed by the Division of Information Technology.
- 3.5 Any security violations and all signs of wrongdoing pertaining to security procedures: Acceptable Use, Internet/Intranet Use, Intrusion Detection, Security

Monitoring and Virus/Malicious Code Protection shall be reported to the University information security officer. Visit <http://wtaccess.wtamu.edu/policies>.

- 3.6 Division/department heads or their equivalents are responsible for ensuring that the WTAMU security program is in effect and that compliance with this rule and standard administrative procedures is maintained for information systems owned and operationally supported by the division/department.
- 3.7 Mission critical or confidential information maintained on an individual workstation or personal computer must be afforded the appropriate safeguards stated in the WTAMU security program and TAC Standards. It is the responsibility of the owner of that workstation or personal computer to ensure that adequate security measures are in place.

\*\*\*\*\*

**CONTACT FOR INTERPRETATION:** Office of Chief Information Officer

APPROVAL:

\_\_\_\_\_  
President/CEO

\_\_\_\_\_  
Date