

24.99.99.W1 Security of Electronic Information Resources

Approved March 8, 2005

Revised July 13, 2010

Supplements System Regulation 29.01.03

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 Texas Administrative Code Title 1, Chapter 202 (TAC 202) "Information Security Standards." The TAC 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 TAC 202 has been delegated by the president to the chief information officer (CIO).

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 WTAMU 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 WTAMU function and for determining controls and access to electronic information resources supporting that WTAMU 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.

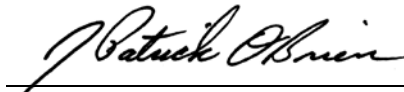
- 2.5 ISAAC (Information Security Awareness Assessment and Compliance) – A web based system used to assess the security posture of information systems and measure compliance with the information security standards. It also provides guides for creating a disaster recovery plan and performing a physical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

3. CONTROLS AND RESPONSIBILITIES

- 3.1 The CIO has designated WTAMU’s information security officer (ISO) as the individual responsible for administering the provisions of this rule and the TAC 202 information security standards.
- 3.2 The ISO shall ensure that, on at least an annual basis, a University-wide electronic information resources security risk management plan and disaster recovery plan are completed. 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 Office of Information Technology (IT), the management of access to WTAMU electronic information resources is delegated to division/department heads or equivalent. The division/department head, director, or equivalent of a department shall be responsible for ensuring that an appropriate security program is in effect and that compliance with this rule and TAC 202 standards is maintained for information systems owned and operationally supported by the department. The WTAMU information resources security standard administrative procedures (SAPs) may be referenced at the following link: <http://www.wtamu.edu/informationtechnology/university-saps-and-rules.aspx>.
- 3.4 The division/department head, director, or equivalent of a department, which provides operational support (custodian) for information systems owned by another WTAMU department, shall have the responsibility for ensuring that an appropriate security program is in effect and that compliance with TAC 202 standards is maintained for the supported information systems.
- 3.5 The ISO 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 IT. The ISO 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 IT.

- 3.6 Any security violations and all signs of wrongdoing pertaining to TAC 202 information security standards shall be reported to the ISO.
- 3.7 All division/department heads, directors or equivalents of a department and designees are responsible for ensuring that the WTAMU security program is in effect and that compliance with this rule and SAPs is maintained for information systems owned and operationally supported by the division/department, director or equivalent for a department. The WTAMU information resources security SAPs may be referenced at the following link: <http://www.wtamu.edu/informationtechnology/university-saps-and-rules.aspx>.
- 3.8 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 202 standards. It is the responsibility of the information resources owner or designee to ensure that adequate security measures are in place and that an annual risk assessment is performed.

CONTACT FOR INTERPRETATION: Chief Information Officer

APPROVAL:  July 13, 2010
President/CEO Date