

UNIVERSITY RULE

24.99.99.M1 Security of Electronic Information Resources

Approved May 27, 2002

Revised May 28, 2009

Rule Statement

It is the responsibility of the information resource owner or designee to ensure that adequate security measures are in place and that an annual risk assessment is performed.

Definitions

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.

Mission Critical Information - Information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

Information Resource Owner – an entity responsible for:

- a business function; and,
- determining controls and access to information resources supporting that business function.

Custodian - A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges.

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.

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.

Official Rule and Responsibilities

1. GENERAL

- 1.1 Texas A&M University's electronic information resources are vital academic 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.
- 1.2 Effective security management programs must be employed to appropriately eliminate or mitigate the risks posed by potential threats to the University's information resources. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction whether accidental or deliberate.
- 1.3 Texas 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 TAC on Information Security Standards has been delegated by the President to the Vice President and Associate Provost for Information Technology.

2. RESPONSIBILITIES

- 2.1 The Vice President and Associate Provost for Information Technology has designated the Information Technology Issues Management (ITIM) group of Networking and Information Security as the entity responsible for administering the provisions of this rule and the TAC Information Security Standards.
- 2.2 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 operationally supported by the department.
- 2.3 The head or director of a department which provides operational support (custodian) for information systems owned by another TAMU 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.

- 2.4 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.
- 2.5 The information resource owner, or their designee, is responsible for ensuring that the risk mitigation measures described in applicable University Rules and Standard Administrative Procedures (SAP) are implemented. Based on risk management considerations and business functions, the resource owner may determine that it would be appropriate to exclude certain risk mitigation measures. All exclusions must be in accordance with SAP 24.99.99.M1.27 Exclusions from Required Risk Mitigation Measures.
- 2.6 Mission Critical or Confidential Information maintained on information resources such as servers, individual workstations, and portable devices must be afforded the appropriate safeguards stated in the TAC Standards and applicable University Rules and Standard Administrative Procedures. It is the responsibility of the information resource owner or designee to ensure that adequate security measures are in place and that an annual risk assessment is performed.

3. COMPLIANCE ASSESSMENT REPORTING

- 3.1 Departments having ownership or custodial responsibility for electronic information systems shall ensure that on an annual basis, a security assessment report is filed with the Office of the Vice President and Associate Provost for Information Technology (via the ISAAC system). This report is produced by the ISAAC system accessed at <http://isaac.tamu.edu/>. The report shall be filed by the designated system administrator or custodian of the information system.
- 3.2 Departments having responsibility for information resources which store, transmit, or process mission critical or confidential information may assess their security posture and measure their compliance with the TAC Information Security Standards by using the Information Security Awareness Assessment and Compliance (ISAAC) system.

Related Statutes, Policies, or Requirements

Texas Administrative Code (TAC) 202 as amended or supplemented

Contact Office

For rule interpretation or clarification, contact Office of the [Vice President and Associate Provost for Information Technology](#).

OFFICE OF RESPONSIBILITY: [Vice President and Associate Provost for Information Technology](#)