Rule Statement
Effective security management programs must be employed to appropriately eliminate or mitigate the risks posed by potential threats to the Texas A&M Engineering Experiment Station (TEES) electronic information resources.

Reason for Rule
This rule allows TEES, as a state agency, to comply with the Texas Administrative Code (TAC) on "Information Security Standards".

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

   1.1 TEES divisions having ownership or custodial responsibility for electronic information systems shall ensure that on an annual basis, division information resources security risk management plan and a disaster recovery plan are sent to the Chief Information Officer. The report shall be filed by the division information security officer or custodian of the information system.

   1.2 The division head or their equivalents 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 division.

   1.3 The division head or their equivalents which provides operational support (custodian) for information systems owned by another TEES division, 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 division head or their equivalents to the appropriate information system support personnel (e.g. System Administrators) within the division.

   1.5 The division heads or their equivalents are responsible for ensuring that the TEES security program is in effect and risk mitigation measures described in
applicable TEES 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 TEES SAP 29.01.99.E1.27, Exclusions from Required Risk Mitigation Measures.

1.6 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 TEES 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.

2. COMPLIANCE ASSESSMENT REPORTING

2.1 Divisions having ownership or custodial responsibility for electronic information systems will ensure that on an annual basis, a security assessment report is filed with the TEES Chief Information Officer (via the Information Security Awareness, Assessment, and Compliance (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.

2.2 Divisions 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 ISAAC system.

Related Statutes, Policies, or Requirements

Information Security Awareness, Assessment, and Compliance (ISAAC) system

TAMU Rule 29.01.99.M1, Security of Electronic Information Resources

TEES SAP 29.01.99.E1.27, Exclusions from Required Risk Mitigation Measures

Contact Office

Information Technology Services
(979) 847-8585