Procedure Statement

Texas A&M University-Commerce’s electronic information resources are vital academic and administrative assets that 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.

Reason for Procedure

This procedure provides guidance for the management and oversight for information security processes.

Procedures and Responsibilities

1. GENERAL

   1.1 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.

   1.2 Texas A&M University-Commerce, as a state university, 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 President. For the purposes of this procedure, 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 Chief Information Officer.

2. RESPONSIBILITIES

   2.1 The president has designated the Information Security Officer of Information Technology responsible for administering the provisions of this procedure 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 procedure 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 A&M-Commerce 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 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 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 Information Security Officer. This report is produced by the Information Security Awareness Assessment and Compliance (ISAAC) system. 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 ISAAC system.

4. INFORMATION SECURITY STANDARDS

4.1 The procedures determining acceptable use of A&M-Commerce information resources are addressed in the following information security standards:

For all campus users

- **Acceptable Use**: Acceptable use of university computing resources
- **Authorized Software**: Standards for licensed software use
- **Email Usage**: Standards for ensuring prudent and acceptable use of email
- **Internet/Intranet Usage**: Acceptable use of university network resources
- **Malicious Code**: Detection and blocking of viruses and spyware
- **Network Access**: Standards for access and use of network infrastructure
- **Password Authentication**: Standards for complexity of passwords and management
### Portable Computing
- **Standards for storage of confidential data stored on mobile computing devices**

### Privacy
- **Conveys the limits and expectations of privacy**

### For network administrators
- **Network Configuration**
  - **Standards for maintenance and expansion and use of network infrastructure**

### For system administrators
- **Account Management**
  - **Standards for administration of user accounts**
- **Administrator/Special Access**
  - **Standards for administration of special access privilege accounts**
- **Backup/Recovery**
  - **Standards for backup and recovery of systems containing essential data**
- **Change Management**
  - **Procedures for modifications of system configuration information**
- **Incident Management**
  - **Describes prevention, detection, and response to security incidents**
- **Intrusion Detection**
  - **Management of the detection of attempts to bypass security**
- **Physical Access**
  - **Management of access to information infrastructure**
- **Security Monitoring**
  - **Ensures security controls are in place and effective**
- **Server Hardening**
  - **Ensures server controls are configured to protect confidential information**
- **Vendor Access**
  - **Require non-University employee to sign non-disclosure form prior to access**

### For system developers
- **System Development**
  - **Process ensuring accurate and efficient system acquisition and/or development**

---

### Related Statutes, Policies, or Requirements

- **System Policy** [29.01 Information Resources](#)
- **System Regulation** [29.01.03 Electronic Information Services Access and Security](#)
- **University Procedure** [29.01.03.R0.01 Information Security Standards Portable Computing](#)

**Supersedes:**
- **University Rule** 24.99.99.R1 Electronic Information Security
- **University Procedure** 24.99.99.R1.01 Electronic Information Security Standards
Definitions

Confidential Information - Information that is excluded 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 Texas A&M University-Commerce 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.

Owner - A person responsible for a university function and for determining controls and access to electronic information resources supporting that university function.

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

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.

Contact Office

Chief Information Officer
903.886.5550