29.01.03 Information Security

Revised September 2, 2016
Next Scheduled Review: September 2, 2021
Click to view Revision History.

Regulation Statement

The Texas A&M System (system) and its members will protect, based on risk, all system and member information and information resources against unauthorized access, use, disclosure, modification or destruction, including assuring the availability, confidentiality and integrity of information. This regulation applies to all information and information resources owned, leased or under the custodianship of any department, operating unit or employee of the agency or institution, including resources outsourced to another institution, contractor or other source such as cloud computing.

Reason for Regulation

This regulation establishes the authority and responsibilities of the system chief information security officer (SCISO) and member information security officers (ISOs) and provides the minimum standards for member information security programs in accordance with the state's *Information Security Standards for Institutions of Higher Education* found in Title 1, Chapter 202, Texas Administrative Code (TAC 202) and other applicable requirements.

Definitions

Click to view Definitions.

Procedures and Responsibilities

1. SYSTEM AND MEMBER INFORMATION SECURITY PROGRAM AND PLANS

   1.1 System Program. The SCISO, as designated by the chancellor or designee, is responsible for coordinating a systemwide information security program under the system chief information officer's (SCIO) supervision, in consultation with member ISOs, and supported by the Security Operations Center (SOC).

   1.2 Member Program. It is each member's responsibility to develop, document and implement an information security program to protect the member's information and information resources, as approved by the member chief executive officer (CEO), the

SCISO, and the SCIO. A member's information security program must contain the elements required by TAC 202, including, but not limited to, the following:

(a) An information security plan as approved by the CEO, SCISO and the SCIO. Each approved plan should be reviewed and updated annually taking into account changes in business, technology, threats, incidents, member mission, etc. The Texas Department of Information Resources' (DIR) Security Control Standards Catalog (Catalog), Section PM-1, also describes the elements of an information security plan.

(b) Annual risk assessments as provided in Section 4.

(c) Appropriate standards and controls to reduce identified risks. Members shall follow the controls outlined in the Catalog. Member standards must be consistent with any system standards developed by the SCISO, in consultation with the member ISOs, and approved by the SCIO.

(d) A process to justify, grant and document exceptions to specific program requirements.

(e) All members must, in consultation with the Information Resources Manager and ISO, identify, define and document the responsibilities of information owners, custodians and users of information resources.

(f) Appropriate submission to DIR of incident reports and biennial information security plans.

(g) Identification of information that is maintained by the member, in centralized and decentralized areas, and outsourced member information.

(h) A documented process for responding to alleged violations of applicable state and federal laws or system or member requirements concerning information security.

1.3 Additionally, members are responsible for implementing a fully operational data loss prevention program. They are also responsible for the timely and complete production and delivery of requested security information and data to the SOC for cyber monitoring purposes.

2. SECURITY OPERATIONS CENTER AUTHORITY AND RESPONSIBILITY

(a) The SOC is a shared service center, funded by the members and serving all members.

(b) The SOC has the ultimate authority to gather and analyze all security information across all members. That is, the SOC will be responsible for coordinating and/or performing all cyber monitoring across the system. This will be carried out in conjunction with the member ISOs' required responsibilities under TAC 202.

(c) The SOC will be responsible for monitoring the wide area network and shall be made aware of all security incidents at member institutions.

(d) Issues identified by the SOC during its cyber monitoring processes will be reported to member ISOs for remediation and reporting purposes. Remediation plans will be submitted by the member ISOs to the CEO, SCIO, SCISO and SOC.

3. INFORMATION SECURITY RESPONSIBILITY AND ACCOUNTABILITY

3.1 Member ISOs. Each member CEO or designee is responsible for designating an ISO who has the explicit authority and duty to administer the information security requirements of TAC 202 across its institution or agency. Each member ISO shall fulfill the detailed responsibilities established by TAC 202, including providing required reports to the CEO and/or DIR. Any report submitted to the CEO or DIR in accordance with TAC 202 shall also be promptly submitted to the SCISO.

3.2 Information Owners. System and member information owners shall fulfill the detailed responsibilities established by TAC 202, and the SCISO and member ISOs will help ensure that information owners have appropriate training, standards, guidance and assistance to comply with these responsibilities.

Significant information owner responsibilities include, but are not limited to:

(a) Inventory and classify information under their authority according to the system's Information Classification Standard, with the concurrence of the CEO or designee; and

(b) Perform the risk assessments provided in Section 1.2, including identify, recommend and document acceptable risk levels for information resources under their authority.

3.3 Information Custodians. System and member information custodians shall fulfill the detailed responsibilities established by TAC 202, and the SCISO, member ISOs and information owners will help ensure that information custodians have appropriate training, standards, guidance and assistance to comply with these responsibilities.

Significant information custodian responsibilities include, but are not limited to:

(a) Implement approved controls and access to information resources under their care; and

(b) Adhere to information security policies and procedures to manage risk levels for information resources.

3.4 Users of Information Resources. Users of system and member information resources shall fulfill the detailed responsibilities established by TAC 202, including, but not limited to:

(a) Use the information resources only for the purpose(s) specified by the system/member or information owner;

(b) Comply with information security controls and this regulation, system standards, and applicable member guidelines or standards to prevent unauthorized or accidental disclosure, modification or destruction; and

(c) Formally acknowledge that they will comply with system and member information security requirements in a method determined by the CEO or designee.

Users of system or member information resources who fail to comply with this regulation and/or system and member information security requirements are subject to disciplinary action, up to and including termination of employment.

4. ANNUAL RISK ASSESSMENT

Each member shall annually conduct and document an information security risk assessment on the member's information and information systems as required by TAC 202. These assessments shall be presented to the member ISO. The purpose of the annual risk assessment is to identify, evaluate and document the level of impact on a member's mission, functions, image, reputation, assets or individuals that may result from the operation of the member's information systems.

5. SECURITY AWARENESS EDUCATION AND TRAINING

Each member shall deliver information security awareness training for all users.

Related Statutes, Policies, or Requirements

The Texas A&M University System Information Security Standards

Security Control Standards Catalog

1 Tex. Admin. Code Ch. 202, Subch. C, *Information Security Standards for Institutions of Higher Education*

Prior to the October 2009 version, this regulation was published as Regulation *21.01.06.*

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

System Chief Information Security Officer
(979) 458-6433