29.01.03 Information Security

Revised February 5, 2018
Next Scheduled Review: February 6, 2023
Click to view Revision History.

Regulation Summary

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.

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) which is operated by System Offices. All references to SOC refer to the System Offices 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 6.

(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.

(i) Ensure the timely and complete production and delivery of security information and data to the SOC and its staff to ensure the sufficient and effective monitoring of the state of cybersecurity for all members.

2. SECURITY OPERATIONS CENTER AUTHORITY AND RESPONSIBILITY

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

2.2 The SOC has the ultimate authority to gather and analyze all security information across all members. All other member cybersecurity operations and activities are responsible for reporting to the SOC. No member cybersecurity operations and activities shall be in conflict with or in competition with the SOC and its operations. The objectives of the SOC supersede all member cybersecurity operations and activities. That is, the SOC will be responsible for coordinating and/or performing all cyber monitoring across the system membership without exception. This will be carried out in conjunction with the member ISOs' required responsibilities under TAC 202.

2.3 The SOC will be responsible for monitoring the wide area network and shall be made aware of all cybersecurity incidents at member institutions.

2.4 In order to foster more effective cybersecurity, the SOC has formed an Information Sharing and Analysis Organization (ISAO) that gathers, aggregates and analyzes cyber monitoring data from among the members. The SOC will further join and share anonymized monitoring data that it gathers in its ISAO with other ISAO organizations observing the guidelines set by the ISAO Standards Organization.

2.5 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. RESEARCH SECURITY OFFICE (RSO) AUTHORITY AND RESPONSIBILITY

3.1 The RSO is a shared services center funded by the members, serving all members for the purpose of meeting federal guidelines for securing Controlled Unclassified Information (CUI) associated with federally funded contracts.

3.2 The RSO shall define, establish and authorize information security standards and systems to comply with the requirements of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.*

3.3 The RSO will serve as a resource for members with regard to securing CUI.

3.4 The RSO shall review, assess and validate all secure enclaves proposed by member CIOs, which are established within the system, for compliance with the NIST SP 800-171 requirements.

3.5 The RSO will serve as the Authorizing Official for any secure enclave established within the system and provide attestation of compliance to the Department of Defense Chief Information Officer.

3.6 The RSO will maintain an NIST SP 800-171 compliant, secure enclave for use by system members as a shared service.

3.7 The RSO will manage onboarding and maintain secure access to the system's secure enclave.

3.8 The RSO will provide a reference blueprint, standard operating procedures, and technical assistance for members that choose to establish their own secure enclaves. Any enclave established within the system shall comply with the specifications established in the reference blueprint, the RSO information security standards, and standard operating procedures.

3.9 Standards for maintaining an NIST SP 800-171 compliant, secure enclave have been developed by the RSO and are available for reference as a supplement to this regulation.

4. INFORMATION SECURITY RESPONSIBILITY AND ACCOUNTABILITY

4.1 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. ISOs are responsible, along with the member CIO, to follow the Notification Matrix, which is a standard that is contained within this regulation and is available to all members.

4.2 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 Data 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.

4.3 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.

4.4 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.

5. SYSTEM MEMBERS

5.1 The security of information that is classified as Confidential under the Data Classification Standard, referenced under this regulation, is an important information asset to information owners, custodians, and to the system overall. As such, each member shall provide an additional cybersecurity protocol and service to protect this kind of information through the use of Multi-Factor Authentication (MFA). This will ensure that only appropriate individuals have access to confidential information. Requests for

exceptions to inclusion in the use of MFA must be approved in advance by and reported annually to the SCISO.

5.2 Distributed computing has historically been a great asset to individual departments and member units since it allows for increased flexibility and the ability to customize solutions. However, risk mitigation balances that customization with the need to:

- Simplify member infrastructure operations;
- Provide additional security of information resources;
- Provide more cost effective computing and storage services;
- Increase the level of disaster recovery services;
- Increase the ability to ensure security compliance and configuration; and
- Provide increased visibility into information compute and storage costs.

Each member shall consolidate all of its significant IT equipment into a centralized member data center(s) or approved commercial data center as soon as practically possible but no later than September 1, 2019. "Significant IT equipment" includes, but is not limited to, mass storage, large/complex computational environments, most virtualized or physical-based servers, and any other internet exposed services. A member may request exceptions for certain equipment, such as specialized lab or research equipment. Each centralized member data center shall provide colocation services and fully managed services for member departments and units. At a minimum, each data center must have: redundant power delivery, redundant networks, redundant cooling, and physical and cybersecurity, and may also provide operating system setup and administration (including virtualized), backup and recovery, storage management, configuration and patch management, and other managed services. All requests for exceptions to the requirements of this section, including requests to extend the deadline, must be approved in advance by the chancellor and reported on an annual basis to the SCISO.

6. 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.

7. 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