29.01.03 Information Security

Revised September 13, 2021
Next Scheduled Review: September 13, 2026
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 under the state's *Information Security Standards for Institutions of Higher Education* found in Title 1, Texas Administrative Code Chapter 202 (TAC 202) and other applicable requirements.

Definitions

Click to view Definitions.

Regulation

1. SYSTEM INFORMATION SECURITY PROGRAM

   1.1 The SCISO, as designated by the chancellor or designee, is responsible for coordinating and monitoring 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 the System Offices. All references to SOC refer to the System Offices SOC.

   1.2 The Texas A&M System Cybersecurity Control Standards Catalog (A&M System Catalog) provides system member agencies and institutions with system-specific implementation guidance for alignment with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls and the Texas Department of Information Resources Security Control Standards Catalog (DIR Catalog).

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 authority to gather and analyze all security information across all members. All other member cybersecurity operations are responsible for reporting and providing all requested security information to the SOC. No member cybersecurity operations or activities are to conflict with the SOC and its operations. The SOC is responsible for coordinating and/or performing all cyber monitoring across the system membership; this is conducted in conjunction with the member ISOs' required responsibilities under TAC 202.

2.3 While the SOC is responsible for monitoring the wide area network, if a member detects any security incident the SOC must be made aware of the incident as soon as possible.

2.4 In order to facilitate effective cybersecurity information sharing, the SOC gathers, aggregates and analyzes cyber monitoring data from among the members. The SOC further aggregates and shares anonymized monitoring data that it gathers with other information sharing and analysis organizations (ISAO), including the State of Texas ISAO, observing the guidelines set by the ISAO Standards Organization.

2.5 Issues identified by the SOC during its cyber monitoring processes are reported to member ISOs for remediation and reporting purposes. Member ISOs must provide a response to the member chief information officer/information resources manager (CIO) and SOC for each issue identified, including a remediation plan to address the identified issue, or justification explaining why a remediation plan is not needed (e.g., false positive detections, acceptable behavior). Remediation plans for issues affecting high impact information resources, as defined in 1 TAC §202.1 are also approved by the member chief executive officer (CEO) and information copied to the SCISO and SCIO.

3. SYSTEM MEMBER INFORMATION SECURITY PROGRAM AND PLANS

It is each member ISO's responsibility to develop, document and implement an information security program to protect the member's information and information resources, in consultation with the member CIO, SCISO and SCIO, and as approved by the member CEO. A member's information security program must include the elements required by TAC 202 Subch. C, in addition to the following system-specific elements:

(a) An institution-wide information security plan approved by the member CEO, in consultation with the SCISO and SCIO. Each approved plan is reviewed and updated annually considering changes in business, technology, threats, incidents, member mission, etc.

(b) Appropriate information security policies, procedures, and controls to address the institution's identified security risks. Members must follow the control standards outlined in the DIR and A&M System Catalogs, and develop controls consistent with those standards catalogs.

(c) A documented process to ensure annual risk assessments are performed and documented by information owners as outlined in Section 6.

(d) A documented process to review the institution's inventory of information and information systems maintained by the member, in both centralized and decentralized areas or outsourced to third-party vendors, and related ownership and responsibilities.

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

(f) The prompt production and delivery of all requested security information to the SOC to ensure sufficient and effective monitoring of the state of cybersecurity for all members.

4. SYSTEM MEMBER INFORMATION SECURITY RESPONSIBILITIES

4.1 Member ISOs. Each member CEO or their 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. Any report sent to the member CEO or DIR per TAC 202 must also be promptly sent to the SCISO. In addition to the urgent incident reporting procedures outlined in TAC §202.73(b)(1), member ISOs and/or CIOs must also follow the incident reporting standard contained in the A&M System Catalog control IR-6.

4.2 Staff Responsibilities. System and member information owners, custodians, and users must fulfill the detailed responsibilities established by TAC §202.72, and the SCISO and member ISOs will help ensure that information owners, custodians, and users have appropriate training, standards, guidance, and assistance to comply with these responsibilities. 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 MEMBER INFORMATION SECURITY PROGRAM ELEMENTS

5.1 Multi-Factor Authentication. Each member must employ the use of Multi-Factor Authentication (MFA) on information resources containing information categorized as Confidential under A&M System Catalog control RA-2 to ensure that only appropriate individuals have access to confidential information. Requests for exceptions to the use of MFA must be approved in advance by and reported annually to the SCISO.

5.2 Data Center Consolidation. Each member must consolidate all significant IT equipment into a centralized member data center(s) or approved commercial data center. "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. Each centralized member data center must provide colocation services and fully managed services for member departments and units. At a minimum, each data center must have:

(a) redundant power delivery;
(b) redundant networks;
(c) redundant cooling; and
(d) adequate physical and cybersecurity,

and may also provide:

(a) operating system setup and administration (including virtualized);

(b) backup and recovery;

(c) storage management;

(d) configuration and patch management; and

(e) other managed services.

A member may request exceptions for certain equipment, such as specialized lab or research equipment. All requests for exceptions to the requirements of this section must be approved in advance by the chancellor and reported on an annual basis to the SCISO.

5.3 Resilient Information System Backup. The ability of a member to effectively recover from a business-interrupting cyber incident depends on the resiliency and availability of the member's backup infrastructure. Each member must ensure that all high impact information resources are protected by a backup strategy which uses one or more of the following:

(a) immutable backup storage, or

(b) a backup process that runs out-of-band, such as through an endpoint backup and recovery agent, preventing direct access to backup storage from the member's production networks,

as soon as possible but no later than September 1, 2022. Members must test their backup strategy at least annually through a restoration of high impact information resources to a non-production computing environment, in addition to the contingency plan testing required by A&M System Catalog control CP-4.

5.4 Commodity Information Technology (IT) Services. Effective, centralized governance and management of information technology is achieved through the elimination of duplicative commodity services that increase the risk profile of the institution. Such commodity IT services include data centers, networks, email, identity and access management, security infrastructure, and cloud-based Software as a Service (SaaS). To ensure members can satisfy compliance and governance requirements associated with the delivery of commodity IT services, each member CIO must explicitly define and authorize the commodity IT services that may be used and/or delivered by the member institution.

6. ANNUAL RISK ASSESSMENT

6.1 Each member must annually conduct and document an information security risk assessment on the member's information and information systems as required by TAC 202. These assessments must 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.

6.2 Members must promptly send to the SOC an inventory of networks containing information resources assessed as high impact following each annual risk assessment.

7. SECURITY AWARENESS EDUCATION AND TRAINING

Each member must deliver information security awareness training for all users. Member ISOs must ensure the member's training program for employees who use a computer to complete at least 25 percent of their required job duties is an approved program as required by Tex. Govt. Code §2054.519.

Related Statutes, Policies, or Requirements

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

Texas Department of Information Resources Security Control Standards Catalog

The Texas A&M University System Cybersecurity Control Standards

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

System Chief Information Security Officer
(979) 458-6450