29.01.03 Information Security

Revised August 28, 2024
Next Scheduled Review: August 28, 2029
Click to view Revision History.

Regulation Summary

The Texas A&M University System (system) and its members must 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 a member, including resources provided by another member, contractor, or other source such as a cloud service provider.

This regulation establishes the authority and responsibilities of the system chief information security officer (SCISO) and member chief information security officers (CISO) and information security officers (ISO) 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 (1 Tex Admin. Code Ch. 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 developing, maintaining, coordinating and monitoring a systemwide information security program under the SCIO's supervision, in consultation with CISOs and ISOs, and supported by Texas A&M System Cybersecurity (A&M System Cybersecurity), an entity of the System Shared Services Center.

   1.2 The Texas A&M System Security Control Standards Catalog (A&M System Catalog) provides members with a system-specific implementation of the Texas Department of Information Resources (DIR) Security Control Standards Catalog. The A&M System Catalog includes minimum information security requirements for all members' information and information resources and standards to be used by all members to provide levels of information security according to risk categorizations. Implementation

of and compliance with applicable security controls listed in the A&M System Catalog is required under this regulation.

2. A&M SYSTEM CYBERSECURITY AUTHORITY AND RESPONSIBILITY

2.1 A&M System Cybersecurity is a shared service center, funded by and serving system members, which includes:

2.1.1 The Office of the CISO, providing strategic cybersecurity management and oversight;

2.1.2 A&M System Cyber Operations, delivering managed cyber monitoring, detection and incident response services, and

2.1.3 Statewide Cybersecurity Services, delivering cyber risk management, information sharing and analysis, and other shared services.

2.2 A&M System Cybersecurity has the authority to:

(a) gather and analyze all cybersecurity-relevant data from members;

(b) coordinate and perform cyber monitoring, detection and incident response among all members;

(c) coordinate, direct and/or perform the deployment of cyber countermeasures among all members as deemed necessary by the SCIO or SCISO;

(d) contract individually with members to provide additional cybersecurity services as required by the members; and

(e) share anonymized data with other information sharing and analysis organizations (ISAO), including the state of Texas ISAO, observing the guidelines set by the ISAO Standards Organization.

2.3 No member cybersecurity operations or activities may conflict with or duplicate services delivered by A&M System Cyber Operations.

2.3.1 Member cybersecurity and IT operations organizations are responsible for promptly providing all requested cybersecurity-relevant data to A&M System Cybersecurity.

2.3.2 Member universities wishing to operate a student-focused university security operations center that supports the experiential learning of cybersecurity curriculum delivered by the university must function as an extension of the A&M System Cyber Operations. Before implementation, the university will coordinate the execution and operation of a university security operations center with A&M System Cybersecurity.

2.4 A&M System Cybersecurity will report issues identified during cyber monitoring to member point(s) of contact for remediation and reporting purposes.

2.4.1 When an identified issue affects or potentially affects the security of research activities subject to System Policy *15.05*, A&M System Cybersecurity will include the System Research Security Office in the notification process.

2.4.2 Member CISO/ISOs must provide a response to A&M System Cybersecurity for each issue identified but not remediated by A&M System Cyber Operations, including a remediation plan to address the identified problem, 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 must be approved by the member chief information officer (CIO) and chief executive officer (CEO), and information copied to the SCISO and SCIO.

3. SYSTEM MEMBER INFORMATION SECURITY RESPONSIBILITIES

3.1 Member CISO/ISOs. Each member CEO or their designated representative is responsible for designating an employee of the system member as CISO. The CISO must have information security duties as their primary duty and the explicit authority and duty to administer the information security requirements of 1 Texas Administration Code 202.71 across the member.

3.1.1 Alternatively, each CEO or their designated representative of a system member who contracts for the management of its Information Security Governance, Risk and Compliance (GRC) program is responsible for designating an employee of the system member as ISO. The ISO should have information security duties as their primary duty and have the explicit authority and duty to administer the information security requirements of 1 Texas Administration Code 202.71 not otherwise delegated in a statement of work to the GRC program provider.

3.1.2 The vice chancellors for agriculture and life sciences and engineering may designate a single agency employee as CISO for all agencies under the management of the respective vice chancellor. The CISO will have information security duties as their primary duty and the explicit authority and duty to administer the information security requirements of 1 Texas Administration Code 202.71 across their responsible agencies.

3.1.3 Any report sent to the member CEO or DIR as required by 1 Texas Administration Code 202.73 must also be promptly submitted to A&M System Cybersecurity via the A&M System ISAO Portal.

3.1.3.1 Security incidents that qualify for reporting to DIR under 1 Texas Administration Code 202.73(d)(1) must also follow A&M System Incident Reporting Guidelines and A&M System Catalog control IR-6.

3.1.3.2 Reports submitted to DIR via the Statewide Portal for Enterprise Cybersecurity Threat, Risk, and Incident Management (SPECTRIM) other than security incident reports referenced in 3.1.3.1 are exempt from this requirement.

3.2 Staff Responsibilities. Information owners, custodians and users must fulfill the detailed responsibilities established by 1 Texas Administration Code 202.72.

3.2.1 The SCISO and member CISO/ISOs will help ensure that information owners, custodians, and users have appropriate training, standards, guidance, and assistance to comply with these responsibilities.

3.2.2 Users of 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. SYSTEM MEMBER INFORMATION SECURITY PROGRAM AND PLANS

4.1 It is each member CISO/ISO's responsibility to develop, document, implement, and maintain an information security program that includes protections based on risk for all information and information resources owned, leased or under the custodianship of any department, operating unit or employee of the member, including outsourced resources to another institution of higher education, contractor or other sources (e.g., cloud computing). The program will be developed in consultation with the member CIO, SCISO and SCIO, and approved annually by the member CEO.

4.2 A member's information security program must include the elements required by 1 Texas Administration Code 202.74 in addition to the following system-specific elements:

(a) A biennial information security plan (the "Plan") prepared following 1 Texas Administration Code 202.73(b), approved by the member CEO in consultation with the member CIO, SCISO and SCIO, and acknowledged by the member's executive leadership (to include, at a minimum, the CEO, chief financial officer, and the executive responsible for institutional compliance). The Plan should consider changes in business, technology, threats, incidents, member mission, etc.

(b) Appropriate information security policies, procedures and controls to address the member's identified security risks. Members must adopt the control standards outlined in the A&M System Catalog and implement, at a minimum, those controls designated as required by DIR and/or A&M System. Members may employ more stringent control standards per 1 Texas Administration Code 202.76(e).

(c) Documented processes to:

(1) annually review the member's inventory of information systems and related ownership and responsibilities;

(2) biennially perform and document a control assessment following A&M System Catalog control CA-2;

(3) perform and document a risk assessment following 1 Texas Administration Code § 202.75 and A&M System Catalog control RA-3 at least:

(i) annually, for high-impact information resources;

(ii) biennially, for other information systems containing confidential data, and

(iii) triennially, for all remaining information systems;

(4) perform and document a penetration test following Texas Government Code 2054.516(a)(2) and A&M System Catalog control CA-8:

(i) prior to implementing a website or mobile application that processes confidential information, and

(ii) an external network penetration test at least biennially;

(5) ensure the prompt delivery of an inventory of member high-impact information resources to A&M System Cybersecurity via the following each annual risk assessment and other information resources as requested;

(6) respond to alleged violations of applicable state and federal laws or system or member requirements concerning information security;

(7) immediately notify A&M System Cyber Operations of any suspected or actual cyber incident affecting a member's high-impact information resource, and

(8) promptly produce and deliver all requested cybersecurity-relevant data to A&M System Cybersecurity to ensure adequate monitoring of the state of cybersecurity for all members.

5. SYSTEM MEMBER INFORMATION SECURITY PROGRAM ELEMENTS

5.1 Data Center Consolidation.

5.1.1 Each member must consolidate all significant IT equipment into a centralized member or approved commercial data center following the requirements of A&M System Catalog control PE-18.

5.1.2 Each centralized member data center must provide colocation and fully managed services for member departments and units.

5.1.3 A member may request exceptions for specific equipment such as specialized lab or research equipment. The chancellor must approve all data center colocation exception requests in advance and the member must report active exceptions annually to the SCISO.

Related Statutes, Policies, or Requirements

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

System Regulation *02.02.01, Vice Chancellor for Agriculture and Life Sciences and Vice Chancellor for Engineering*

System Regulation *02.04, System Members of The Texas A&M University System*

System Policy *15.05, System Research Security Office*

Tex. Gov't. Code §2054.516, *Data Security Plan for Online and Mobile Applications*

The Texas A&M University System Cybersecurity Standards

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

Cybersecurity
(979) 458-6433