

29.02.01 Information Security Governance



Revised [March 25, 2026](#)

Next Scheduled Review: March 25, 2031

Click to view [Revision History](#).

Regulation Summary

This regulation establishes the information security program governance framework, and roles and responsibilities for implementing information security controls (security controls) throughout The Texas A&M University System (system). The system chief information security officer (SCISO) performs an annual review of this regulation and makes updates as necessary to ensure alignment with new federal and state of Texas (state) policy, mandates, standards, and guidance. All system members (members) must adhere to this regulation and may develop supplemental rules and procedures if necessary to address specific member needs.

This regulation applies to all system information and information resources that collect, process, transmit, store, and disseminate system information including contractor-managed, cloud services, and systems leveraged from other federal and state agencies. Members must hold employees, contractors, guest researchers, collaborators, and individuals with access to system information and information resources accountable for adhering to this regulation.

References to system information and information resources in this regulation apply equally to System Offices-owned and member-owned information and information resources.

Definitions

Click to view [Definitions](#).

Regulation

1. ROLES AND RESPONSIBILITIES

- 1.1 System Chief Information Security Officer. The chancellor or designated representative is responsible for designating an employee of the System Offices as the SCISO. The SCISO is responsible for serving as the central focal point and enforcing system-wide cyber and information security management while providing oversight on the implementation of state cyber and information security requirements, in consultation with member chief information officers (CIOs) and information security officers (ISOs).
- 1.2 Member Information Security Officer. Each member chief executive officer (CEO) or their designated representative is responsible for designating an employee of the member as an ISO or chief information security officer (CISO).

- 1.2.1 Members that do not outsource or contract with another system member to manage the governance, risk, and compliance (GRC) aspect of its information security program must designate a CISO who has information security duties as their primary duty and the explicit authority and duty to administer the information security requirements of Title 1, Texas Administration Code Section 202.71 across the member.
- 1.2.2 Members that do outsource or contract with another system member to manage the GRC aspect of its information security program must designate an ISO who should have information security duties as their primary duty and has the explicit authority and duty to administer the information security requirements of 1 Texas Administration Code Section 202.71 across the member. The ISO is responsible for monitoring the performance of the outsourced or contracted GRC program provider.
- 1.2.3 The vice chancellors for agriculture and life sciences, engineering, and disaster and emergency services may designate a single agency employee as CISO for all agencies under the management of the respective vice chancellor. The CISO has information security duties as their primary duty and the explicit authority and duty to administer the information security requirements of 1 Texas Administration Code Section 202.71 across their responsible agencies.
- 1.2.4 Reports transmitted to the member CEO, Texas Department of Information Resources (DIR), or Texas Cyber Command (TCC) required by 1 Texas Administration Code Section 202.73 must also be promptly submitted to the System Office of Cybersecurity (OCS) in the manner prescribed.
- 1.3 Texas A&M System Cybersecurity. Texas A&M System Cybersecurity is a shared service center, funded by, and serving system members, which includes:
 - 1.3.1 OCS, providing strategic cybersecurity management and oversight; and
 - 1.3.2 Texas A&M System Cyber Operations, delivering managed cyber monitoring, detection and incident response, cyber engineering, and cyber engagement services.
- 1.4 Staff Responsibilities. Information owners, custodians, and users must fulfill the detailed responsibilities established by 1 Texas Administration Code Section 202.72. Users of system information resources who fail to comply with cyber and information security policies, regulations, the information security controls matrix (ISCM), standards, or member rules or procedures are subject to disciplinary action up to and including termination of employment.

2 INFORMATION SECURITY PROGRAM REQUIREMENTS

- 2.1 The system information security program is continuously evaluated to ensure its policies, regulations, ISCM, standards, and guidelines align with federal and state requirements. The use of automation should be incorporated wherever possible; and members must implement and manage security control requirements to avoid, detect, counteract, and minimize security risks to physical property, information, information resources, and privacy of information or other assets.

- 2.2 The system information security governance framework serves as the foundation for the information security program. This regulation and the associated information security controls matrix (ISCM), standards, and guidelines collectively provide flexibility for the information security program to adapt to evolving threats and effectively manage risks. This framework includes:
- 2.2.1 **Regulations** as the primary mechanism to enforce information security requirements and define roles and responsibilities.
 - 2.2.2 **ISCM** to supplement policy and regulations by identifying organizationally defined control parameters, in accordance with 1 Texas Administration Code Section 202.76 and the Security Control Standards Catalog published by the Texas Department of Information Resources.
 - 2.2.3 **Standards** based on the ISCM with specific technical requirements for information security.
 - 2.2.4 **Guidelines** to guide the implementation of processes in support of the policy, regulation, and standards.
- 2.3 The Texas A&M System Security Control Standards Catalog (A&M System Catalog) provides members with a system-specific implementation of the Security Control Standards Catalog published by the Texas Department of Information Resources. The A&M System Catalog, combined with the control family requirements outlined in section 2.4, establishes minimum information security requirements for all system information and information resources. Implementation of and compliance with the required controls identified in the ISCM is required under this regulation.
- 2.4 Security Control Families.
- 2.4.1 Incident Response (IR). Texas A&M System Cyber Operations is the central authority for the system's incident handling, response, reporting, and management of security incidents. In support of these functions, members are responsible for providing security monitoring, auditing, and security incident-related data to Texas A&M System Cyber Operations. Members must:
 - (a) Establish an incident handling support capability that includes adequate preparation, detection and analysis, containment, eradication and recovery, post-incident, and user response activities in coordination with Texas A&M System Cyber Operations;
 - (b) Track, document, and report security incidents to Texas A&M System Cyber Operations;
 - (c) Follow the guidance of Texas A&M System Cyber Operations for incident handling;
 - (d) Support Texas A&M System Cyber Operations by providing information necessary to support security incident investigation upon request;
 - (e) Provide training to employees and contractors on incident reporting and response activities; and

- (f) Not duplicate or conflict with services delivered by Texas A&M System Cyber Operations.
- 2.4.2 Physical and Environmental Protection (PE). System information resources hosted on-premises must implement physical and environmental security controls at the hosting facility. Members must document approval by the member CIO and ISO for each hosting facility.
- 2.4.3 Planning (PL). The System Security Plan (SSP) is critical to ensuring security controls that are planned or in place are adequately documented. Members must create, document, review, and update annually (at a minimum) an SSP for each system information resource that is high-impact or contains confidential information.
- 2.4.4 Program Management (PM). The program management (PM) controls are essential for establishing minimum security requirements necessary to support the system's information security program. To reduce the burden on member assessment and authorization activities, where appropriate, OCS will coordinate with responsible entities to implement, assess, manage, and offer for inheritance applicable controls as a system common controls program. Members must:
- (a) Develop, document, implement, and maintain an information security program and associated member rules and procedures, and controls to address the member's identified security risks. The program will be developed in consultation with the member CIO and approved annually by the member CEO;
 - (b) Prepare a biennial information security plan using the format provided by the Texas Cyber Command, approved by the member CEO in consultation with the member CIO and SCISO, 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., and
 - (c) Annually review the member's inventory of information systems and related ownership and responsibilities and submit the inventory to OCS in the manner prescribed.
- 2.4.5 Risk Assessment (RA). A member's system information resources must have a documented risk assessment in accordance with policies, regulations, ISCM, standards, member rules and procedures, and guidelines. The risk assessment must be consistent with the security categorization of the information resource and impact to the confidentiality, integrity, and availability of the data the information resource stores, processes, and transmits. Members must:
- (a) Perform penetration testing on websites or mobile applications that process confidential information prior to implementing the information resource; and
 - (b) Periodically assess the risk to member's system information resources, at

least:

- (i) Annually, for high-impact information resources;
- (ii) Biennially, for other information resources containing confidential information; and
- (iii) When significant configuration changes occur for all remaining information systems.

2.4.6 System and Services Acquisition (SA). The procurement of tools, technologies, and services must adhere to the system procurement policy, which takes into consideration the impact on the system's mission. Members must:

- (a) Demonstrate a business justification for the procurement, along with allocation of sufficient resources to protect system information and information resources;
- (b) Perform supply chain risk assessments and ensure supply chain risk management processes are in place for acquisitions of information resources that are high-impact or contain confidential information;
- (c) Implement software usage and installation restrictions on system information resources and comply with applicable copyright laws and licensing agreements;
- (d) Hold third-party providers contractually accountable to comply with policies, regulations, ISCM, standards, member rules and procedures, and guidelines; and
- (e) Ensure outsourced services employ adequate continuous monitoring to protect the confidentiality, integrity, and availability of system information and information resources.

Related Statutes, Policies, or Requirements

[Texas Government Code Ch. 2063, *Texas Cyber Command*](#)

[Title 1, Texas Administrative Code Ch. 202, subch. C, *Information Security Standards for Institutions of Higher Education*](#)

[System Policy 02.03, *System Administration*](#)

[System Policy 02.04, *System Members of The Texas A&M University System*](#)

[System Policy 24.01, *Risk Management*](#)

[System Policy 29.01, *Information Resources*](#)

[System Policy 32.02, *Discipline and Dismissal of Employees*](#)

[System Policy 33.04, Use of System Resources](#)

[System Regulation 02.02.01, Vice Chancellor for Agriculture and Life Sciences and Vice Chancellor for Engineering](#)

[System Regulation 25.07.03, Acquisition of Goods and/or Services](#)

[Texas A&M University System Cybersecurity Standards and Guidelines](#)

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

Cybersecurity
(979) 234-0030