29.02 Information Security

Approved February 5, 2026 (MO -2026)
Next Scheduled Review: February 5, 2031

Policy Summary

The Board of Regents (board) of The Texas A&M University System (system) regards cyber and information security as vital to fulfilling the mission of the system. The system chief information security officer (SCISO) is responsible for coordinating the system's cyber and information security, including ensuring, in consultation with each member chief executive officer (CEO), the confidentiality, integrity and availability of system members' (member) information resources.

References to system information and information resources in this policy applies equally to System Offices-owned and member-owned information and information resources.

Policy

1. In accordance with Chapter 2063, Texas Government Code, the system maintains an information security program that facilitates the protection of system information resources and operations. The System Office of Cybersecurity (OCS) establishes the governance framework, policy requirements, and standards for managing the security of system information resources.

2. While information security and privacy are independent disciplines, both are closely related, therefore it is essential for the system to take a coordinated approach in identifying and managing risks. OCS provides oversight on the system information security program while the System Office of Ethics & Compliance and member privacy officers, in coordination with OCS, serves as the central authority for privacy within the system.

3. OCS serves as the central focal point and enforces system-wide information security management while providing oversight on the implementation of State of Texas (state) cyber and information security requirements. To strengthen the system's information security posture, OCS and members must continue collaborating to support the business functions of the system.

4. The system information security program defines goals for and delegates information security responsibility to the members. These goals represent baseline expectations for the system's information security posture, taking into consideration the respective business needs and missions of each member. The adoption of a system common controls program and enterprise security architecture will result in more efficient and effective implementation of security requirements.

5. The system information security governance framework serves as the foundation for the information security program. This policy and associated regulations, 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:

   5.1 **Regulations** as the primary mechanism to enforce information security requirements and define roles and responsibilities.

   5.2 **ISCM** to supplement policy and regulations by identifying organizationally defined control parameters, in accordance with Title 1, Texas Administrative Code, Section 202.76 and the Texas Security Control Standards Catalog.

   5.3 **Standards** based on the ISCM with specific technical requirements for information security.

   5.4 **Guidelines** to guide the implementation of processes in support of the policy, regulation, and standards.

6. The concepts found within the Texas Cybersecurity Framework (TCF), NIST Risk Management Framework (RMF), and NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, comprise the basis for the system's information security program. The information security program provides a formal, structured approach for developing risk assessments for information resources and provides a uniform standard for evaluating security risks to information resources operating by or on behalf of the system. The primary focus of this approach must be on the information resource's business purpose, not on the specific IT resource. The effective management of risks is essential to protecting the information and information resources that enable the system's critical mission.

7. The system should embrace a forward-leaning enterprise security architecture which entails transitioning away from legacy systems and adopting modern and emerging technologies. Members must collaborate with OCS to reduce the system's legacy IT footprint, evaluate emerging technologies, and assess opportunities for integration to achieve enterprise solutions whenever possible.

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

System Policy 24.01, *Risk Management*

System Policy 29.01, *Information Resources*

System Regulation 29.02.01, *Information Security Governance* (in progress)

Member Rule Requirements

A rule is not required to supplement this policy.

Contact Office

Cybersecurity
(979) 234-0030