29.01.03 Information Security

Revised August 28, 2024
~~Revised September 12, 2022~~

Next Scheduled Review: ~~September 12, 2027~~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 (~~TAC~~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 ~~system chief information officer's (~~SCIO's~~)~~ supervision, in consultation with ~~member chief information security officers (~~CISOs~~)~~ and ISOs, and supported by Texas A&M System Cybersecurity (A&M System Cybersecurity), an entity of the ~~Security Operations Center (SOC) which is operated by the system~~System Shared Services Center~~. All references to SOC refer to the system SOC~~.

   1.2 The Texas A&M ~~University~~ System ~~Cybersecurity~~Security Control Standards Catalog (A&M System Catalog) provides members with a system-specific ~~guidance for~~

~~implementing controls in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls and~~implementation of the Texas Department of Information Resources ~~Security Control Standards Catalog~~ (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 ~~SECURITY OPERATIONS CENTER~~CYBERSECURITY AUTHORITY AND RESPONSIBILITY

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

2.1.1 The Office of the CIS~~C~~O,~~hief Information Security Officer~~ providinge~~s~~ strategic cybersecurity ~~situational awareness, cybersecurity~~ management and oversight; ~~.~~

2.1.2 A&M System Cyber Operations, deliverings~~s~~ managed cyber monitoring, detection and incident response services, and ~~.~~

~~2.1.0~~2.1.3 Statewide Cybersecurity Services, deliverings~~s~~ cyber ~~threat~~risk management, information sharing and analysis, and ~~intelligence to all members.~~ other shared services.

2.2 ~~The SOC~~A&M System Cybersecurity has the authority to:

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

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

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

~~(b)~~(d) contract individually with members to provide~~perform~~ additional cybersecurity ~~operations functions~~ services as required~~needed~~ by the members; and~~,~~ ~~and~~

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

2.3 No member cybersecurity operations or activities may conflict with ~~the SOC and its operations~~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 ~~security information~~ requested ~~by the SOC to the SOC in a timely manner~~cybersecurity-relevant data to A&M System Cybersecurity.

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

2.4 ~~The SOC reports~~A&M System Cybersecurity ~~–~~will report~~s~~ issues identified during ~~cybersecurity~~cyber monitoring to member ~~CISO/ISOs~~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~~, the SOC also informs~~ in the ~~Research Security Office (RSO) of the identified issue for RSO follow-up~~notification process.

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

3. ~~–~~SYSTEM MEMBER INFORMATION SECURITY RESPONSIBILITIES

3.1 Member CISO/ISOs.

~~3.1.1~~ Each member CEO or ~~designee~~ their designated representative is responsible for designating an employee of the system member as ~~Chief Information Security Officer (~~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 ~~section §~~ 202.71 across the member.

3.1.1 Alternatively, each CEO or their designated representative of a system member ~~that does not contract with a third party~~who contracts for the management of its Information Security Governance, Risk~~,~~ and Compliance (GRC) program is responsible for designating an employee of the ~~member as CISO. The CISO is primarily responsible for the member's information security program and has the explicit authority and duty to administer the information security requirements of 1 TAC § 202.71 on behalf of the member.~~

~~3.1.2 Each~~system member ~~CEO or designee of a member that contracts with a third party for the management of its Information Security GRC program is responsible for designating an employee of the member as~~ as ~~Information Security Officer (~~ISO~~.).~~ The ISO ~~is primarily responsible for the member's~~should have information security ~~program~~ duties as their primary duty and ~~has~~have the explicit

authority and duty to administer the information security requirements of 1 ~~TAC~~Texas~~.~~ Administration~~.~~ Code ~~section~~§ 202.71 ~~on behalf of the member~~ not otherwise delegated in a statement of work to the GRC program provider.

3.1.~~3~~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 ~~is primarily responsible for those agencies'~~will have information security ~~programs~~duties as their primary duty and ~~has~~ the explicit authority and duty to administer the information security requirements of 1 ~~TAC~~Texas~~.~~ Administration ~~.~~Code ~~section~~§ 202.71 ~~on behalf of those~~across their responsible agencies.

~~3.1.4 Except for the monthly incident reports submitted to the Texas Department of Information Resources (DIR) pursuant to 1 TAC § 202.73(b)(2), any~~3.1.3 Any report sent to the member CEO or DIR as required by 1 ~~TAC~~Texas~~.~~ Administration~~.~~ Code ~~section~~§ 202.73 must also be promptly ~~sent to the SCISO. The member must also follow the incident reporting standard contained in~~ submitted to A&M System ~~Catalog control IR-6 for any such incidents~~Cybersecurity via the ~~TAMUS~~A&M System ISAO Portal.

3.1.3.1 Security incidents that qualify for reporting to DIR ~~in accordance with~~under 1 ~~TAC §~~ Texas~~.~~ Administration~~.~~ Code~~section~~§ 202.73(~~b~~d)(1) must also follow ~~the incident reporting standard~~A&M System Incident Reporting Guidelines ~~contained in~~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. ~~System and member information~~Information owners, custodians~~,~~ and users must fulfill the detailed responsibilities established by 1 ~~TAC~~Texas~~.~~ Administration~~.~~ Code ~~section~~§ 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 ~~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.

4. SYSTEM MEMBER INFORMATION SECURITY PROGRAM AND PLANS

4.1 It is each member CISO/ISO's responsibility to develop, document, ~~and~~ implement, and maintain an information security program ~~to protect the member's~~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 ~~as~~ approved annually 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:~~

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

(a) A biennial information security plan (the "Plan") prepared ~~in accordance with~~following 1 Texas~~.~~ ~~Gov't~~Administration ~~.~~ Code ~~§ ection 2054.133,~~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 (~~including~~to include, at a minimum, the ~~member's~~ CEO, chief financial officer, and the executive responsible for institutional compliance). ~~Each approved~~The ~~P~~plan ~~is reviewed and updated biennially in conjunction with the Texas DIR-required Information Security Plan, considering~~should consider changes in business, technology, threats, incidents, ~~and/or~~ member mission, etc.

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

(c) ~~A documented process~~Documented processes to ~~ensure annual~~:

(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 ~~assessments are performed and documented in accordance with 1 TAC~~assessment following 1 Texas~~.~~ Administration~~.~~ Code § 202.75 and A&M System Catalog control RA-3~~.~~ at least:

(i) ~~A documented process~~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~~'s~~ Code ~~section~~§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;

~~(4)~~(5) ensure the prompt delivery of an inventory of member ~~assets containing~~ high~~-~~impact information resources~~, as defined in 1 TAC § 202.1,~~ to ~~the SOC~~A&M System Cybersecurity via the~~TAMUS~~ following each annual risk assessment~~.~~ and other information resources as requested;

(c) A documented process to review the member'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.

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

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

(7)(8) promptly produce and deliver all requested cybersecurity-relevant informationdata to the SOCA&M System Cybersecurity to ensure sufficient and effectiveadequate monitoring of the state of cybersecurity for all members.

5. SYSTEM MEMBER INFORMATION SECURITY PROGRAM ELEMENTS

5.1 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 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:

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

(b) backup and recovery;

(c) storage management;

(d) configuration and patch management; and

other colocation and fully managed services. for member departments and units.

5.1.3 A member may request exceptions for certainspecific equipment, such as specialized lab or research equipment. AllThe chancellor must approve all data center colocation exception requests forin advance and the member must report active exceptions to the requirements of this section must be approved in advance by the chancellor and reported on an annual basisannually to the SCISO.

5.2 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 member. 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 are delivered centrally by the member.~~

Related Statutes, Policies, or Requirements

1 Tex. Admin. Code Ch. 202, s~~S~~ubch. 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~~

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.~~as~~ Gov~~ernmen~~'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

~~System Chief Information Technology~~Cybersecurity~~Security Officer~~
(979) 458-~~6450~~6433