29.01.99.D1 Information Resources

Approved: March 28, 2016
Revised: May 1, 2019
January 29, 2025
Next Scheduled Review: January 29, 2030

Rule Summary

Texas A&M University-Central Texas (A&M-Central Texas) regards information resources as vital academic and administrative assets that are required to fulfill the mission of the university. The chief executive officer (President) is ultimately responsible for ensuring the confidentiality, security and efficiency of A&M-Central Texas' information resources.

This rule establishes the authority and responsibilities of the President, what the President delegates to the Chief Information Officer (CIO), the Information Security Officer (ISO), and outlines the procedures that govern the use of information resources at A&M-Central Texas as required by System Policy *29.01, Information Resources.*

Rule

1. INFORMATION RESOURCES GOVERNANCE

1.1 The president must designate an Information Resource Manager (IRM) pursuant to 1 Tex. Admin. Code Ch. 211. The president designates the CIO to serve as the IRM.

1.2 Pursuant to 1 Tex. Admin. Code Ch. 202 and System Regulation *29.01.03, Information Security* (Section 4.1), the president must designate an ISO who has the explicit authority and duty to administer information security requirements in consultation with The Texas A&M University System (A&M System) Chief Information Security Officer (SCISO).

1.3 Under the direction of A&M-Central Texas administration, the CIO and ISO must establish an information resources governance structure that:
(a) Identifies and coordinates the best source(s) of information technology hardware, software and services.
(b) Reduces non-productive redundancy across A&M-Central Texas.
(c) Consolidates resources including networks, hardware, systems, and applications as appropriate.
(d) Ensures the security of A&M-Central Texas's technology, infrastructure, and information resources.

2. INFORMATION RESOURCES SECURITY

2.1 The President is ultimately responsible for the security of state information resources.

2.2 In accordance with System Policy *29.01, Information Resources* and System Regulation *29.01.03, Information Security*, the CIO and the ISO will:

(a) Work within the A&M-Central Texas governance and compliance environment to develop all required rules, procedures and guidelines to ensure compliance with applicable laws, policies and regulations regarding information resources and security. This includes the development of an A&M-Central Texas information security program (System Policy *29.01, Information Resources*, Section 2.3, and System Regulation *29.01.03, Information Security*, Section 1.2).

(b) Ensure that appropriate training, guidance and assistance is available to information owners, custodians, and users.

(c) Conduct annual information security risk assessments.

(d) Conduct annual security awareness education and training.

3. ACCESSIBILITY OF ELECRONIC AND INFORMATION RESOURCES

3.1 All faculty and staff must comply with TAC 206.70, TAC 213, this rule, and related guidelines in the development, procurement, maintenance, or use of electronic and information resources (EIR) and web content.

3.2 The president must designate an EIR Accessibility Coordinator (EIRAC) to ensure compliance with this rule. In the absence of this designation, the CIO will serve as the EIRAC. Any request for an exception under TAC 213 must be submitted to the EIRAC for review and processing.

3.3 Compliance Plan

(a) The EIRAC, CIO, and Procurement Coordinator and Manager of Enrollment Marketing Systems & Web Initiatives must develop an EIR Accessibility Implementation Plan under which all new and existing EIRs and web content will be brought into compliance with TAC 206.070 and TAC 213.

(b) The EIR Accessibility Implementation Plan must guide compliance with this rule and detail and keep current EIR accessibility training, monitoring, and procurement guidelines.

(c) The EIRAC, CIO, and Procurement Coordinator and Manager of Enrollment Marketing Systems & Web Initiatives must oversee and provide training on compliance with TAC 206.70, TAC 213, this rule, and the EIR Accessibility Implementation Plan.

3.4 Exceptions

(a) The EIRAC must review requests for exceptions under TAC 213, ensure that requests meet the requirements for an exception, and forward requests to the CIO with a recommendation for approval or disapproval.

(b) The CIO will serve as the presidents designees for the approval of exception requests as indicated in the EIR Accessibility Implementation Plan.

(c) The EIRAC will maintain exception requests by the Texas A&M University System Records Retention Schedule.

3.5 Monitoring

(a) The Procurement Coordinator and EIRAC must monitor purchasing contracts, purchase orders, and procurement card purchases for compliance with TAC 213, this rule, and procurement procedures related to EIR.

(b) The Manager of Enrollment Marketing Systems & Web Initiatives and EIRAC must monitor web content for compliance with TAC 206.70 and this Rule.
(c) The EIRAC and the CIO must oversee and monitor the development, support, and maintenance of EIR and compliance with this rule and A&M-Central Texas wide compliance with TAC 206.70 and TAC 213.

3.6 The CIO, Procurement Coordinator, and Manager of Enrollment Marketing Systems & Web Initiatives will support the necessary technical and procurement procedures to the EIRAC in fulfilling their responsibilities under this Rule.
(a) Ensure that appropriate training, guidance and assistance is available to information owners, custodians and users.
(b) Conduct annual information security risk assessments.
(c) Conduct annual security awareness education and training.

4. USE OF INFORMATION RESOURCES

4.1 Each user of an information resource is responsible for using A&M-Central Texas information resources in accordance with the guidelines established by applicable System policies and regulations, and agency rules, procedures and standards.

4.2 There is no expectation of privacy when using A&M-Central Texas information resources beyond that which is expressly provided by applicable privacy laws.

4.3 A&M-Central Texas reserves the right to limit, restrict, or deny privileges and access to its information resources for those who violate A&M-Central Texas Rules and Standard Administrative Procedures, A&M System Policies and Regulations, and/or relevant local, state, federal, and international laws.

Related Statutes, Policies, or Requirements

1 Tex. Admin. Code Ch. 202, *Information Security Standards*

1 Tex. Admin. Code Ch. 206, *State Websites*

1 Tex. Admin. Code Ch. 211, *Information Resources Managers*

1 Tex. Admin. Code Ch. 213, *Electronic and Information Resources*

System Policy *29.01 Information Resources*

System Regulation *29.01.03 Information Security*

System Regulation *29.01.04 Accessibility of Electronic and Information Resources*

System Policy *33.04 Use of System Resources*

The Texas A&M University System Information Security Standards

Contact Office

Information Technology
(254) 519-5426