29.01.99.R1 Information Resources

Approved: May 19, 2025
Next Scheduled Review: May 19, 2030

Rule Summary

East Texas A&M University (University) regards information resources as vital academic and administrative assets required to fulfill the university's mission. The Chief Information Officer (CIO) and Chief Information Security Officer (CISO)/Information Security Officer (ISO) are responsible for ensuring the confidentiality, security, and efficiency of university information resources.

This rule establishes the authority and responsibilities of the CIO and the CISO/ISO and outlines the procedures that govern the use of information resources at the University as required by System Policy *29.01, Information Resources*.

Procedures and Responsibilities

1 INFORMATION RESOURCES GOVERNANCE

1.1 The CIO will serve as the Information Resource Manager (IRM) under Title 1, Chapter 211 of the Texas Administrative Code (TAC) unless the president delegates otherwise.

1.2 Under 1 TAC 202 and System Regulation *29.01.03, Information Security* (Section 4.1), the president must designate a CISO/ISO who has the explicit authority and duty to administer information security requirements in consultation with The Texas A&M University System Chief Information Security Officer (SCISO). The University reserves the right to limit, restrict or deny privileges and access to its information resources for those who violate University rules and procedures, The Texas A&M University System (System) policies and regulations, and/or relevant local, state, federal, and international laws.

1.3 Under the direction of the University administration, the CIO and CISO/ISO must establish an information resources governance structure that:

1.3.1 Identifies and coordinates the best source(s) of information technology hardware, software and services;

1.3.2 Reduces non-productive redundancy across the University;

1.3.3 Consolidates resources, including networks, hardware, systems, and applications as appropriate; and

1.3.4 Ensures the security of University technology infrastructure and information resources.

2 INFORMATION RESOURCES SECURITY

Following System Policy *29.01, Information Resources*, and System Regulation *29.01.03, Information Security*, the CIO and the CISO/ISO will:

2.1 Work within the University 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 developing a University information security program (System Policy *29.01, Information Resources*, Section 2.3, and System Regulation *29.01.03, Information Security*, Section 1.2).

2.2 Ensure appropriate training, guidance and assistance are available to information owners, custodians and users.

2.3 Conduct annual information security risk assessments.

2.4 Conduct annual security awareness education and training.

3 ACCESSIBILITY OF ELECTRONIC AND INFORMATION RESOURCES

3.1 All faculty and staff must comply with 1 TAC 213, this rule and related guidelines (University Procedure *29.01.04.R0.01 Accessibility Requirements for Electronic and Information Resources*) in developing, procuring, maintaining, or using electronic and information resources (EIR).

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 must serve as EIRAC. Any request for an exception under 1 TAC 213 must be submitted to the EIRAC for review and processing.

3.3 Compliance Plan

3.3.1 The EIRAC, CIO, and Director of Purchasing & Support Services must develop an EIR Accessibility Implementation Plan under which all new and existing EIRs will comply with 1 TAC 213.

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

3.3.3 The EIRAC, CIO, and Director of Purchasing & Support Services must oversee and provide training on compliance with 1 TAC 213, this rule, and the EIR Accessibility Implementation Plan.

3.4 Exceptions

3.4.1 The EIRAC must review requests for exceptions under 1 TAC 213, ensure that requests meet the requirements for an exception, and forward requests to the CIO with a recommendation for approval or disapproval.

3.4.2 The CIO must serve as the president's designee to approve exception requests.

3.4.3 The EIRAC must maintain exception requests by System Records Retention Schedule.

3.5 Monitoring

3.5.1 The Director of Purchasing & Support Services and EIRAC must monitor purchasing contracts, purchase orders, and procurement card purchases for compliance with 1 TAC 213, this rule, and procurement procedures related to EIR.

3.5.2 The EIRAC and the CIO must oversee and monitor the development, support, and maintenance of EIR, compliance with this rule, and University compliance with 1 TAC 213.

3.6 The CIO and Director of Purchasing & Support Services must support the necessary technical and procurement procedures to the EIRAC in fulfilling their responsibilities under this rule.

4 INDIVIDUAL RESPONSIBILITY FOR INFORMATION RESOURCES

4.1 The University utilizes numerous official social networks and social media sites to communicate with students, alumni, and the community. All accounts must follow the University's and the System's established guidelines for social media. All employees are reminded that established internal communication channels should be the primary professional form of communication for addressing employee concerns specific to the University, its administration, faculty, staff, or programs. At all times, University employees should ensure that their personal social networks and social media posts are not construed as endorsed by, originating from, or representing the University, its administration, faculty, staff, or programs—and are instead posted by a private individual.

4.2 Faculty members who utilize social networks or social media sites for classroom instruction must comply with all provisions of the Family Educational Rights and Privacy Act.

4.3 Recreational use of personal social networks and social media sites must be avoided during work hours and comply with System Policy *33.04, Use of System Resources.* There is no expectation of privacy when using university information resources beyond that which is expressly provided by privacy laws.

4.4 When representing the University on social media, including through the operation of a university-affiliated account, employees must maintain the same standards of conduct expected of all faculty and staff, namely, being respectful, helpful and informative. Social media activity on behalf of the University should promote university initiatives and values.

Related Statutes, Policies, or Requirements

Tex. Gov't Code Ch. 2054, *Information Resources*

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 *33.04, Use of System Resources*

System Regulation *29.01, Information Resources*

System Regulation *29.01.03, Information Security*

The Texas A&M University System Cybersecurity Policy

University Procedure 29.01.04.R0.01, Accessibility Requirements for Electronic and Information Resources

Definitions

Information resources – the procedures, computer equipment, computing facilities, software, and data purchased, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, report, and transmit information.

Information Resources Manager (IRM) — The individual designated by the executive head or deputy executive head of an institution of higher education to be responsible for the day-to-day management of information resources in the institution.

Information Security Officer (ISO) — The individual designated by the institution of higher education per Texas Government Code §2054.136 to have explicit authority for information security for the entire organization.

Contact Office

Center for IT Excellence
903.468.6000
ISO@etamu.edu