UNIVERSITY RULE

29.01.99.M1 Information Resources

Approved June 10, 2024
Next scheduled review: June 10, 2029

Rule Statement

The Texas A&M University System (system) regards information resources as a vital part of fulfilling the mission of the university. The chief executive officer (CEO) is ultimately responsible for the management and security of state information resources. The chief information officer (CIO) is responsible for day-to-day management of the university's information resources. In addition, the CIO, in coordination with the chief information security officer (CISO), is responsible for ensuring that appropriate procedures and programs are implemented to safeguard computer systems, networks and data; and to mitigate risks that may compromise information integrity, availability and security.

This rule implements System Policy 29.01, establishes the authority and responsibilities of the CIO and the CISO, and authorizes procedures and standards governing the use and security of information resources within the university.

Definitions

- **Information resources** – the procedures, computer equipment, computing facilities, software and data which are 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 in accordance with Texas Government Code §2054.136 to have explicit authority for information security for the entire organization.

Official Procedures and Responsibilities

1. UNIVERSITY INFORMATION RESOURCES GOVERNANCE

1.1. In accordance with Texas Administrative Code, Title 1, section 211.20, the CEO shall designate an Information Resources Manager (IRM); thus, the CEO designates the chief information officer (CIO) as the IRM to administer the requirements of Texas Administrative Code, Title 1, Part 10 and all other relevant information resources laws and policies across the university.

1.2. The efficient and effective use of information resources is critical to the long-term success of the university. To that end, the CIO is responsible for ensuring that information resources expenditures from any funding source are efficient and serve to improve university services. The CIO is also responsible for coordinating university information resources purchases, regardless of the funding source.

1.3. The CIO, with the CEO's approval, must establish an information resources governance structure for the university that accomplishes the following:

1.3.1. addresses IT issues that impact the entire university through a formalized mechanism for input and recommendations;

1.3.2. ensures that IT aligns with the outcomes required by the university for the successful fulfillment of its mission;

1.3.3. ensures that appropriate decision-making activities are done in concert with the university's strategic priorities; and

1.3.4. reviews and provides recommendations on proposed information technology projects while considering input from a broad base of stakeholders.

1.4. The CIO must develop and implement University Rules, Standard Administrative Procedures, and Security Controls as necessary to ensure compliance with Texas Administrative Code, Title 1, Part 10.

2. UNIVERSITY INFORMATION SECURITY GOVERNANCE

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

2.2. In accordance with Texas Administrative Code, Title 1, section202.71 and Texas Administrative Code section 2054.136, the CEO designates the chief information security officer (CISO) as the Information Security Officer to administer the information security requirements of Texas Administrative Code, Title 1, Part 10 and all other relevant information security laws and policies across the university.

2.3. The CISO must develop and implement University Rules, Standard Administrative Procedures, and Security Controls to ensure compliance with applicable federal, state and system information security statutes, policies and regulations; including Texas Administrative Code, Title 1, Chapters 202, 206, and 213, and Texas Government Code section 2054.

2.4. Mandatory security controls required by Texas Administrative Code, Title 1, Section 202.76 and System Regulation *29.01.03* must be defined by the CISO in a security control catalog published on the university's website. University security controls carry the same force and effect as university rules, and noncompliance may be considered grounds for disciplinary action up to and including termination of employees.

Related Statutes, Policies, or Requirements

Tex. Gov't Code Ch. 2054, *Information Resources*
1 Tex. Admin. Code Part 10, *Department of 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*
Texas A&M Information Security Controls Catalog
System Policy *29.01*, *Information Resources*
System Regulation *29.01.01*, *Information Resources Governance*
System Regulation *29.01.03*, *Information Security*

Contact Office

Office of the Chief Information Security Officer
Technology Services
(979)-458-1342