

29.01.01.N1 Information Resources

Approved: Awaiting OGC approval
Next Scheduled Review: February 26, 2023



Rule Summary

This rule implements [System Policy 29.01](#), establishes the authority and responsibilities of the chief information officer (CIO) and information security officer (ISO), and authorizes procedures and standards governing the use and security of information resources within the agency.

Rule Statement

The Texas A&M Engineering Extension Service (TEEX) regards information resources as a vital part of fulfilling the mission of the agency. The chief information officer (CIO) is responsible for coordinating the agency's information resources, including ensuring, in consultation with the chief executive officer (CEO) or designee, the effectiveness, security and efficiency of the agency's information resources. In addition, the CIO, in consultation with the CEO or designee, 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.

Definitions

- **1 TAC**—Title 1, Texas Administrative Code, *Administration*.
- **Agency Information Resource**—An information resource owned, leased, managed, or otherwise under the control of the Texas A&M Engineering Extension Service.
- **Chief Executive Officer (CEO)**—The agency director of the Texas A&M Engineering Extension Service; also the head of an institution of higher education as defined by §61.003, Texas Education Code.
- **Chief Information Officer (CIO)**—The individual designated by the CEO to administer the requirements of 1 TAC Part 10 and all other relevant information resources laws and policies across the agency; also the information resources manager as defined by 1 TAC §211.20 and §2054.071, Texas Government Code.
- **Information Owner**—A person with statutory or operational authority for specified information (e.g., supporting a specific business function) and responsibility for establishing the controls for its generation, collection, processing, access, dissemination,

- and disposal. The Information Owner may also be responsible for other information resources including personnel, equipment, and information technology that support the Information Owner’s business function.
- **Information Resources**—Is defined in §2054.003(7), Texas Government Code and/or other applicable state or federal legislation.
- **Information Security Officer (ISO)**—The individual designated by the CEO to administer the information security requirements of 1 TAC Chs. 202 – 203 and all other relevant information security laws and policies across the agency; also defined by 1 TAC §202.71.
- **User of an Information Resource**—An individual or automated application authorized to access an information resource in accordance with the information owner-defined controls and access rules.

Rule

1. AGENCY INFORMATION RESOURCES GOVERNANCE

- 1.1. In accordance with 1 TAC §211.20, the chief executive officer (CEO) designates the chief information officer (CIO), under the supervision of the CEO or designee, as the information resources manager to administer the requirements of 1 TAC Part 10 and all other relevant information resources laws and policies across the agency.
- 1.2. The efficient and effective use of information resources is critical to the long-term success of the agency. To that end, the CIO is responsible for ensuring that information resources expenditures from any funding source are efficient and serve to improve agency services. The CIO is also responsible for coordinating agency information resources purchases, regardless of the funding source.
- 1.3. The CIO, with the CEO’s approval, shall establish an information resources governance structure at the agency level that accomplishes the following:
 - (a) identifies and coordinates information technology projects and their priority among the agency’s division, program and operational areas;
 - (b) reviews and provides recommendations on proposed information technology projects with substantial impact to agency stakeholders;
 - (c) reviews and provides recommendations on proposed information technology capital investment requests; and
 - (d) reviews and provides recommendations on the agency’s information resources strategic plan.

1.4. The CIO shall develop and implement procedures and standards as necessary to ensure compliance with 1 TAC Part 10.

2. AGENCY INFORMATION SECURITY GOVERNANCE

- 2.1. In accordance with 1 TAC §202.70, the CEO designates the information security officer (ISO) to administer the information security requirements of 1 TAC Chs. 202 – 203 and all other relevant information security laws and policies across the agency.
- 2.2. The ISO shall develop and implement procedures and standards to ensure compliance with applicable Federal, State and TAMUS information security rules.
- 2.3. Mandatory security controls required by 1 TAC §202.76 and System Regulation 29.01.03 shall be defined by the ISO in a security control standards document published on the agency's intranet website. Agency security control standards carry the same force and effect as agency rules, and noncompliance may be considered grounds for disciplinary action up to and including termination of employees.

3. USE OF AGENCY INFORMATION RESOURCES

- 3.1. Each user is responsible for using agency information resources in accordance with the guidelines established by applicable System policies and regulations, and agency rules, procedures and standards.
- 3.2. Privacy policies are mechanisms used to establish the responsibilities and limits for system administrators and users in providing privacy in information resources. There is no expectation of privacy when using agency information resources beyond that which is expressly provided by applicable privacy laws. Information created, stored or transmitted on agency information resources may be subject to disclosure under the Texas Public Information Act or through legal or administrative proceedings. While the agency does not routinely monitor individual usage of agency information resources, the agency has the right to examine information created, stored or transmitted on agency information resources for general business purposes, including but not limited to the normal operation and maintenance of such resources.

Related Statutes, Policies, or Requirements

- [1 Texas Administrative Code Part 10, Department of Information Resources](#)
- [1 Texas Administrative Code Ch. 202, Information Security Standards](#)
- [1 Texas Administrative Code Ch. 211, Information Resources Managers](#)
- [Texas Education Code §51.9335, Acquisition of Goods and Services](#)
- [Texas Government Code Ch. 2054, Information Resources](#)

- [System Policy 29.01, Information Resources](#)
- [System Regulation 25.07.03, Acquisition of Goods and/or Services](#)
- [System Regulation 29.01.01, Information Resources Governance](#)
- [System Regulation 29.01.03, Information Security](#)
- Agency Security Control Standards Catalog (Located on TEEXConnect.org)

Contact Office

TEEX Network & Information Services, 979-458-6867