Rule 29.01.99.D1 Information Resources

Approved: October 22, 2015
Revised:
Next Scheduled Review: October 22, 2018

Rule Statement

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 Information Officer (CIO) and the Information Security Officer (ISO) are responsible for ensuring the confidentiality, security and efficiency of the university's information resources.

Reason for Rule

This rule establishes the authority and responsibilities of the CIO and the 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.***

Procedures and Responsibilities

1. INFORMATION RESOURCES GOVERNANCE

   1.1 As an institution of higher education, A&M-Central Texas is required to comply with Texas Administrative Code Ch. 202 (TAC202) and Ch. 211 (TAC211) regarding information resources. TAC202 assigns ultimate responsibility for information resources to the President of the university. Under TAC211 the President may designate a senior official as the designee who functions as the Information Resource Manager (IRM). At A&M-Central Texxas, the IRM role is typically delegated to the University's CIO.

   1.2 Under TAC202 and *System Regulation 29.01.03 Information Security (Section 2.1)* the President shall designate an 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).

1.3 The efficient and effective use of information resources is critical to the long-term success of the University. The CIO and ISO are responsible for ensuring that the University and all information resource owners have implemented the required rules, procedures and guidelines for the appropriate management of information resources under their control.

1.4 Under the direction of the University administration, the CIO and ISO shall 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 the University.
(c) Consolidates resources including networks, hardware, systems and applications as appropriate.
(d) Ensures the security of the University's technology infrastructure and information resources.

2. INFORMATION RESOURCES SECURITY

2.1 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 University's governance and compliance environment to develop all required rules, procedures and guidelines to ensure compliance with applicable laws, policy and regulations regarding information resources and security. This includes the development of the University's 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.

Related Statutes, Policies, or Requirements

1 Tex. Admin. Code Ch. 202, Subch. C, *Information Security Standards for Institutions of Higher Education*
1 Tex. Admin. Code Ch. 211, *Information Resources Managers*
System Policy *29.01, Information Resources*
System Regulation *29.01.03, Information Security*
The Texas A&M University System Information Security Standards

Definitions

TAMUCT Information Technology Glossary

Contact Office

Information Technology, Chief Information Officer
(254) 519-5426