TEXAS A&M **INTERNATIONAL** UNIVERSITY

Rule

29.01.99.L1 Information Resources

First Approved: April 4, 2012 *(formerly Rule 29.01.99.L1, Use of Information Resources and Facilities)*
Revised: September 4, 2017
October 8, 2018
March 19, 2026
Reviewed: July 31, 2023
Next Scheduled Review: March 19, 2031

Rule Statement and Reason for Rule

Texas A&M International University (TAMIU) 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 Chief Information Security Officer (CISO)/the Information Security Officer (ISO) are responsible for ensuring the confidentiality, security, and efficiency of TAMIU's 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 TAMIU as required by System Policy *29.01, Information Resources*, and *System Policy 29.02, Information Security*, and in coordination with The Texas A&M University System Office of Cybersecurity.

Procedures and Responsibilities

1. INFORMATION RESOURCES GOVERNANCE

1.1. The Associate Vice President for Information Technology/CIO will serve as the Information Resource Manager (IRM) under Texas Administrative Code (TAC) Chapter 211 unless otherwise delegated by the President.

1.2. Under System Policy *29.02, Information Security*, System Regulation *29.01.03, Information Security*, (Section 4.1), and applicable state law, including Texas Government Code Chapter 2063, the President will 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 (System) Chief Information Security Officer (SCISO). TAMIU reserves the right to limit, restrict, or deny privileges and access to its information resources for those who violate TAMIU Rules and Standard Administrative Procedures, System Policies and Regulations, and/or relevant local, state, federal, and international laws.

1.3. Under the direction of TAMIU administration, the CIO and CISO/ISO will 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 TAMIU.

(c) Consolidates resources including networks, hardware, systems, and applications as appropriate.

(d) Ensures the security of TAMIU's technology infrastructure and information resources.

2. INFORMATION RESOURCES SECURITY

2.1. The CIO and the CISO/ISO will:

(a) Work within TAMIU 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 TAMIU information security program (System Policy *29.01, Information Resources*, Section 2.3, and System Regulation *29.01.03, Information Security*, Section 1.2), System Policy *29.02, Information Security* and Texas Government Code Chapter 2063.

(b) Ensure that appropriate training, guidance, and assistance are 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 ELECTRONIC AND INFORMATION RESOURCES

TAMIU adheres to TAMUS Regulation, 29.01.04, Accessibility of Digital Resources.

4. INDIVIDUAL RESPONSIBILITY FOR INFORMATION RESOURCES

4.1. TAMIU utilizes numerous official social networks and social media sites as communication channels with students, alumni, and the community. All follow both TAMIU and System-established guidelines for social media. At all times, TAMIU employees should ensure that their posts are not construed as endorsed by, originating from, or representing TAMIU, its administration, faculty, staff, or programs—and are instead posted in the employee's capacity. All employees are reminded that established internal communication channels are available to address employee concerns specific to TAMIU, its administration, faculty, staff, or programs, and should be the primary professional channel for such matters.

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 (FERPA), as well as federal and state accessibility laws.

4.3. Recreational use of personal social networks and social media sites is to be avoided during work hours and must comply with System Policy *33.04, Use of System Resources*. Employees do not expect privacy when using TAMIU information resources beyond that which is expressly provided by privacy laws.

4.4. As a representative of TAMIU, employees must maintain the same standards of conduct expected of all faculty and staff, namely being respectful, helpful, and informative. Conversations on social media should enhance civic discussion.

Related Statutes, Policies, or Requirements

TAC, Chapter 202, Subchapter C, Information Security Standards for Institutions of Higher Education
TAC, Chapter 211, Information Resources Managers
TAC, Chapter 213, Subchapter C, Electronic and Information Resources
TGC, Chapter 2063, Texas Cyber Command
System Policy *29.01, Information Resources*
System Regulation *29.01.03, Information Security*
System Regulation *29.01.04, Accessibility of Digital Resources*
System Policy 29.02, Information Security
System Policy *33.04, Use of System Resources*
The Texas A&M University System Information Security Standards

Contact Office

Office of Information Technology, 956-326-2310