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
Reviewed: **July 31, 2023**
Next Scheduled Review: **July 31, 2028**

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

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 TAMIU as required by *System Policy 29.01, Information Resources*.

Procedures and Responsibilities

1. INFORMATION RESOURCES GOVERNANCE

1.1 The Associate Vice President for Information Technology/Chief Information Officer (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 TAC 202 and *System Regulation 29.01.03, Information Security* (Section 4.1), 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). 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, Texas A&M University System Policies and Regulations, and/or relevant local, state, federal, and international laws.

1.3 Under the direction of TAMIU 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 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 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 TAMIU 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 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).
(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.

3. ACCESSIBILITY OF ELECTRONIC AND INFORMATION RESOURCES

3.1 All faculty and staff shall comply with TAC 213, this Rule, and related guidelines in the development, procurement, maintenance, or use of electronic and information resources (EIR).

3.2 The President shall designate an EIR Accessibility Coordinator (EIRAC) to ensure compliance with this Rule. In the absence of this designation, the CIO shall serve as EIRAC. Any request for an exception under TAC 213 must be submitted to the EIRAC for review and processing.

3.3 Compliance Plan

(a) The EIRAC, CIO, and Director of Purchasing & Support Services shall develop an EIR Accessibility Implementation Plan under which all new and existing EIR will be brought into compliance with TAC 213.
(b) The EIR Accessibility Implementation Plan must guide compliance with this Rule and detail and keep current EIR accessibility training, monitoring, and procurement guidelines.
(c) The EIRAC, CIO, and Director of Purchasing & Support Services shall oversee and provide training on compliance with TAC 213, this Rule, and the EIR Accessibility Implementation Plan.

3.4 Exceptions

(a) The EIRAC shall review requests for exceptions under TAC 213, ensure that requests meet the requirements for an exception, and forward requests to the CIO with a recommendation for approval or disapproval.
(b) The CIO shall serve as the President's designee for the approval of exception requests.
(c) The EIRAC shall maintain exception requests in accordance with the Texas A&M University System Records Retention Schedule.

3.5 Monitoring

(a) The Director of Purchasing & Support Services and EIRAC shall monitor purchasing contracts, purchase orders, and procurement card purchases for compliance with TAC 213, this Rule, and procurement procedures related to EIR.
(b) The EIRAC and the CIO shall oversee and monitor development, support, maintenance of EIR and compliance with this Rule and TAMIU-wide compliance with TAC 213.

3.6 The CIO and Director of Purchasing & Support Services shall provide the necessary technical and procurement procedures support to the EIRAC in fulfilling his or her responsibilities under this Rule.

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 The Texas A&M University System's established Guidelines for Social Media. At all times, TAMIU employees should ensure that their personal 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 individual capacity. All employees are reminded that there are established internal communication channels to address employee concerns specific to TAMIU, its administration, faculty, staff, or programs which should be the primary professional form of communication on such matters.

4.2 Faculty 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).

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 have no expectation of privacy when using TAMIU information resources beyond that which is expressly provided by privacy laws.

4.4 As a representative of TAMIU, it is imperative employees 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, Regulations, or SAP's

TAC, Chapter 202, Subchapter C, Information Security Standards for Institutions of Higher Education
TAC, Chapter 211, Information Resources Managers
TAC, Chapter 213, Subchapter C, Accessibility Standards for Institutions of Higher Education
System Policy 29.01, Information Resources
System Regulation 29.01.03, Information Security
System Regulation 29.01.04, Accessibility of Electronic and Information Resources
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