University Rule

29.01.99.J1 Information Resources

Approved: October 26, 2026
Next Scheduled Review: October 26, 2031

Rule Summary

Texas A&M University-Victoria (A&M-VICTORIA) 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, integrity, availability, security, and efficiency of the university's information resources. The Digital Accessibility Officer (DAO) is responsible for overseeing the university's compliance with digital accessibility requirements per federal and state regulations.

This rule establishes the authority and responsibilities of the CIO, the ISO, and the DAO and outlines the procedures that govern the use of information resources at A&M-VICTORIA as required by System Policy *29.01, Information Resources.*

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.

Rule

1. INFORMATION RESOURCES GOVERNANCE

   1.1. The President hereby designates the CIO as the Information Resources Manager (IRM) under Texas Administrative Code, Title 1, Part 10, Chapter 211.

   1.2. Under Texas Administrative Code Title 1, Part 10, Chapter 202 and System Regulation *29.01.03, Information Security,* the President will 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). A&M-VICTORIA reserves the right to limit, restrict or deny privileges and access to its information resources for those who violate A&M-VICTORIA rules and procedures, A&M System policies and regulations, and/or relevant local, state, federal, and/or international law.

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

1.4. Under the direction of A&M-VICTORIA administration, the CIO and ISO will establish an information resources governance structure that:

1.4.1. Identifies and coordinates the best source(s) of information technology hardware, software and services.
1.4.2. Reduces non-productive redundancy across A&M-VICTORIA.
1.4.3. Consolidates resources including networks, hardware, systems and applications as appropriate.
1.4.4. Oversees the security of A&M-VICTORIA's technology infrastructure and information resources.

2. INFORMATION RESOURCES SECURITY

2.1. In accordance with System Policy *29.01, Information Resources,* and System Regulation *29.02.01, Information Security Governance,* the CIO and the ISO will:

2.1.1. Work within A&M-VICTORIA'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 A&M-VICTORIA's information security program (System Policy *29.01, Information Resources, Section 2.3* and System Regulation *29.02.01, Information Security Governance, Section 1.2*).

2.1.2. Ensure that appropriate training, guidance and assistance is available to information owners, custodians and users.

2.1.3. Conduct information security risk assessments.

2.1.4. Conduct security awareness education and training.

3. ACCESSIBILITY OF ELECTRONIC AND INFORMATION RESOURCES

3.1. All faculty and staff must comply with the digital accessibility requirements specified in federal and state regulations for any digital resources used to apply for, gain access to, or participate in services, programs, and activities of A&M-VICTORIA (System Regulation *29.01.04, Accessibility of Digital Resources)*

3.2. The President will designate a Digital Accessibility Officer (DAO) to ensure compliance with this rule. In the absence of this designation, the CIO will serve as the DAO.

3.3. Compliance Plan

3.3.1. The DAO develops, publishes, and implements a Digital Accessibility Plan under which digital resources are brought into and maintained in compliance

with the digital accessibility requirements per federal and state regulations, to include a process for corrective actions to remediate non-compliant digital resources.

3.3.2. The DAO, CIO, Purchasing, and Marketing Communication will oversee and provide training on compliance with this rule as well as the Digital Accessibility Plan.

3.4. Reporting

3.4.1. The DAO will conduct and completes DIR's biennial survey and submit reports to compliance offices when required.

3.5. Websites, Web Pages, and Web Applications

3.5.1. The DAO monitors organizational websites, web pages, web applications (including social media and learning management systems), and mobile applications to ensure they meet minimum technical accessibility standards, unless specific exemptions or exceptions are allowed under federal or state regulations.

3.6. Digital Resource Acquisition and Procurement

3.6.1. Information Technology, Purchasing, and the DAO will adhere to requirements related to the solicitation and acquisition of digital products and services to ensure compliance with applicable policies, rules and regulations.

3.7. Risk Management and Accommodations

3.7.1. The DAO will establish and maintain a documented risk management procedure for the development, procurement, maintenance, and use of digital resources that do not conform to federal and state digital accessibility requirements. The procedure must identify and mitigate associated risks, ensure provision of reasonable alternative access, and specify the process for requesting exceptions in accordance with applicable regulations.

3.7.2. Faculty and staff are responsible for coordinating and facilitating auxiliary aids and services to provide reasonable accommodation(s) for qualified individuals with disabilities. This responsibility applies when digital resources do not comply with federal and state digital accessibility requirements or when an access barrier is identified.

3.7.3. Faculty and staff must also follow the university's documented risk management procedure to evaluate risks, provide alternative access, and request exceptions in accordance with applicable regulations.

3.7.4. The university must maintain mechanisms for reporting alleged violations of state or federal accessibility regulations, barriers to access, and other digital accessibility concerns.

3.8. Exceptions and Exemptions

3.8.1. The DAO will develop and implement a procedure that includes maintaining a record of applicable exemptions and approved exceptions.

3.8.2. Exceptions to the Digital resources must be approved by the President or their designee.

3.8.3. The DAO or their designee can utilize system-wide approved exceptions at the university's discretion or execute university specific exceptions approved by the President or their designee.

3.8.4. The DAO will maintain exception requests in accordance with the university's record retention schedule.

3.9 The DAO oversees and monitors development, support, maintenance, and compliance with this rule and DIR accessibility requirements.

Related Statutes, Policies, or Requirements

Title II of the Americans with Disabilities Act of 1990 (ADA)

Section 504 of the Rehabilitation Act of 1973

Section 508 of the Rehabilitation Act of 1973

Texas Labor Code Chapter 21, Employment Discrimination

1 Tex. Admin. Code Ch. 477, 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*

Tex. Gov't. Code 2054, Subchapter M., Access to Electronic and Information Resources by Individuals with Disabilities

System Policy *29.01, Information Resources*

System Regulation 29.02.01, Information Security Governance

System Regulation *29.01.04, Accessibility of Digital Resources*

Contact Office

Information Technology
(361)-570-4399