29.01.99.C1 Security of Electronic Information Resources

Revised: July 10, 2023
Next Scheduled Review: July 10, 2028
Revision History

Rule Summary

This rule is required by Texas A&M University System policy *29.01, Information Resources* and outlines 1) information-security governance at Texas A&M University-Corpus Christi (TAMU-CC) and 2) the process for the creation and maintenance of Information Technology (IT) standards.

Rule

1. GENERAL

    1.1. The electronic information resources of TAMU-CC are vital academic and administrative assets which require appropriate safeguards. Computer systems, networks, and data are vulnerable to a variety of threats. These threats have the potential to compromise the integrity, availability, and confidentiality of university information.

    1.2. Effective security management programs must be employed to appropriately eliminate or mitigate the risks posed by potential threats to the university's information resources. Measures must be taken to protect these resources against unauthorized access, disclosure, modification, or destruction, whether accidental or deliberate.

    1.3. The university, as a state institution of higher education, is required to comply with Title 1, Chapter 202 of the Texas Administrative Code (TAC 202), *Information Security Standards*. TAC 202 assigns responsibility for protection of informational resources to the President.

2. REQUIREMENTS

2.1. Per system regulation *29.01.03, Information Security*, the President designates the Chief Information Security and Privacy Officer (CISPO), under the supervision of the Associate Vice President & Chief Information Officer (CIO), to administer the information security requirements of TAC 202 and all other relevant information security laws and policies across the institution.

2.2. The CISPO may issue binding and enforceable IT policy in the form of documented IT standards. IT standards must not be used to document the broad rights and responsibilities of all users, which must be documented in university rules and procedures. The CISPO presents proposed IT standards and proposed changes to or deletions of existing IT standards to the CIO and the IT senior staff for feedback. After review and incorporation of any appropriate feedback the CISPO sends the proposal to the University Technology Council, the Vice President for Finance & Administration, and all IT staff, who have 10 business days to respond. The CISPO provides any proposed edits submitted during the 10-day response period are provided to the CIO and IT senior staff for additional feedback. CISPO will review all proposed edits and feedback over 10 business days and accept or reject for incorporation in the proposal. Upon CISPO approval the proposal becomes official and is posted on a website accessible to all university users. The CISPO reviews all IT standards at least annually.

Related Statutes, Policies, or Requirements

Texas Administrative Code, Chapter 202
System Policy *29.01, Information Resources*
System Regulation *29.01.03, Information Security*
University IT Standard Acceptable Use
University IT Standard Cybersecurity Control Standards Catalog and Appendix A

Contact Office

Contact for clarification and interpretation: Office of Information Security
(361) 825-2124