29.01.99.C1 Security of Electronic Information Resources

Approved June 1, 2016
Reviewed June 1, 2016
Next Scheduled Review June 1, 2018

Rule Statement

This Rule defines 1) information-security governance at TAMUCC and 2) the process for the creation and maintenance of IT Standards.

Reason for Rule

This Rule is required by Texas A&M University System Policy 29.01, Section 2.3.

Procedures and Responsibilities

1.   GENERAL

    1.1   The electronic information resources of Texas A&M University – Corpus Christi ("University") 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 the 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 shall 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 the Texas Administrative Code ("TAC"), in particular, TAC Chapter 202 "Information Security Standards." TAC 202 assigns responsibility for protection of informational resources to the President.

2.   RULES

     2.1   Per System Regulation 29.01.03, Section 2.1, the President designates the Information Security Officer ("ISO"), under the supervision of the Associate Vice President for Information Technology/Chief Information Officer ("CIO"), to administer the information-security requirements of TAC 202, and all other relevant information-security law and policy, across the institution.

     2.2   The ISO may issue binding and enforceable IT policy in the form of documented IT Standards. The ISO will present proposed IT Standards and proposed changes to or deletions of existing IT Standards ("proposal(s)") to the CIO and the IT Senior Staff. If the proposal is approved by a simple majority of the CIO and the IT Senior Staff, then the ISO will send the proposal to the University Technology Counsel, the Executive Vice-President of Finance and Administration, and all information technology staff, who will have 10 working days to respond. Any edits submitted during the 10-day response period will be accepted or rejected based on a simple majority vote of the CIO and IT Senior Staff. At the end of the 10-day period the proposal will become official and will be posted on a website accessible to all University users. The ISO will review all IT Standards at least annually. IT Standards shall not be used to document the broad rights and responsibilities of all users; these shall be documented in either a Procedure or a Rule.

Related Statutes, Policies or Requirements

System Policy 29.01 Information Resources
System Regulation 29.01.03 Information Security
University Standard IT Standards for All Users
University Standard IT Standards for Owners and Custodians (login required)

Contact Office

Contact for Interpretation: Office of Information Security (361) 825-2124