29.01.99.E1 Security of Electronic Information Resources

Supplements Policy 29.01, Regulation 29.01.03

Rule Statement
Texas A&M Engineering Experiment Station and the Texas A&M University College of Engineering (Texas A&M Engineering) regards electronic information resources as a vital part of fulfilling the mission of the institution. Texas A&M Engineering has consolidated their respective IT infrastructure into one system. Therefore, for efficient security operations, combined infrastructure will be under a single set of security practices and controls. Texas A&M Engineering reserves the right to implement supplemental controls or new rules to address unforeseen or future conditions.

Reason for Rule
This Rule supplements System Policy 29.01, establishes the authority and responsibilities of the Chief Information Officer (CIO) and Information Security Officer (ISO), and authorizes procedures and standards governing the use and security of information resources.

Procedures and Responsibilities

1. INFORMATION RESOURCES GOVERNANCE

1.1 In accordance with 1 TAC §211.20, the agency director designates the Chief Information Officer (CIO), under the supervision of the agency director or designee, as the information resources manager to administer the requirements of 1 TAC Part 10 and all other relevant information resources laws and policies.

1.2 The efficient and effective use of information resources is critical to the long-term success of Texas A&M Engineering. To that end, the CIO is responsible for ensuring that information resources expenditures from any funding source are efficient and serve to improve information resources services. The CIO is also responsible for coordinating information resources purchases, regardless of the funding source.

1.3 The CIO, with the agency director’s approval, shall establish an information resources governance structure that accomplishes the following:
(a) identifies and coordinates information technology projects and priorities;
(b) reviews and provides recommendations on proposed information technology
   projects that have substantial impact to relevant stakeholders;
(c) reviews and provides recommendations on proposed information technology
capital investment requests; and
(d) reviews and provides recommendations on information resources strategic
   plans.

1.4 The CIO shall develop and implement procedures and standards as necessary
to ensure compliance with 1 TAC Part 10.

2. INFORMATION SECURITY GOVERNANCE

2.1 In accordance with 1 TAC §202.70, the agency director designates the
   Information Security Officer (ISO). The ISO, under the supervision of the CIO,
   will administer the information security requirements of 1 TAC 202 and 203 as
   well as all other relevant information security laws and policies.

2.2 The ISO shall develop and implement procedures and security control standards
to ensure compliance with applicable Federal, State and Texas A&M University
   System (TAMUS) information security requirements (including export controls,
classified information, and controlled unclassified information).

2.3 Mandatory security controls required by 1 TAC §202.76 and System Regulation
   29.01.03 shall be defined by the ISO in a security control standards document
   published on an internally accessed website. These security control standards
   carry the same force and effect as applicable policies and rules. Noncompliance
   may be considered grounds for disciplinary action up to and including termination
   of employees.

3. USE OF INFORMATION RESOURCES

3.1 Each user is responsible for using information resources in accordance with the
guidelines established by applicable policies, regulations, rules, procedures and
   standards.

3.2 Privacy policies are mechanisms used to establish the responsibilities and limits
   for system administrators and users in providing privacy for information
   resources. There should be no expectation of privacy when using Texas A&M
   Engineering information resources beyond that which is expressly provided by
   applicable privacy laws. Information created, stored or transmitted on Texas
   A&M Engineering information resources may be subject to disclosure under the
   Texas Public Information Act or through legal or administrative
   proceedings. While individual usage of information resources is not routinely
   monitored, designated Texas A&M Engineering information resources personnel
   have the authority to examine information created, stored or transmitted on
Texas A&M Engineering information resources, including but not limited to the normal operation and maintenance of such resources.

**Related Statutes, Policies, or Requirements**

- Policy 29.01, Information Resources
- Regulation 15.99.02, Classified Information
- Regulation 25.07.03, Acquisition of Goods and/or Services
- Regulation 29.01.01, Information Resources Governance
- Regulation 29.01.03, Information Security
- Texas Education Code §51.9335, *Acquisition of Goods and Services*
- Texas Government Code Ch. 2054, *Information Resources*
- 1 Texas Administrative Code Part 10, *Department of Information Resources*
- 1 Texas Administrative Code Ch. 202, *Information Security Standards*
- 1 Texas Administrative Code Ch. 211, *Information Resources Managers*
- Texas DIR Security Control Standards Catalog
- Texas A&M Engineering Security Control Standards Catalog

**Definitions**

1 TAC—Title 1, Texas Administrative Code, *Administration*.

**Contact Office**

Engineering Information Technology
(979) 847-8585