1. GENERAL

1.1 Texas A&M University-Corpus Christi’s electronic information resources 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 Texas A&M University-Corpus Christi, as a state university, is required to comply with the Texas Administrative Code (TAC) on “Information Security Standards.” (See Texas Administrative Code Chapter 202.) The Texas Administrative Code assigns responsibility for protection of informational resources to the President. For the purposes of this rule, the authority and responsibility regarding the University’s compliance with the Texas Administrative Code on Information Security Standards has been delegated by the President to the Assistant Vice President for Technology.

2. DEFINITIONS

2.1 Confidential Information - Information that is excepted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal laws. Most student records are confidential records.

2.2 Mission Critical Information - Information that is defined by Texas A&M University-Corpus Christi or any division thereof (department, etc.), to be essential to their function(s) and would cause severe detrimental impact if the data/system were lost and unable to be restored in a timely fashion.

2.3 Owner - A person responsible for a University function and for determining controls and access to electronic information resources supporting that University function.

2.4 Custodian - A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges.

2.5 An appropriate security assessment software system is used to assess the security posture of information systems and measure compliance with the Information Security Standards. It also provides guides for creating a disaster recovery plan and performing a physical security check. Additionally, a security training course (information and test) is provided.

3. RESPONSIBILITIES

3.1 The Assistant Vice President for Technology is designated as the Information Technology (IT) security officer and is the person responsible for administering the provisions of this rule, Texas A&M System IT security policies, and the Texas Administrative Code (TAC) Information Security Standards.

3.2 The head or director of an administrative unit shall be responsible for ensuring that an appropriate security program is in effect and that compliance with this rule and TAC standards is maintained for information systems owned and operationally supported by the department.

3.3 The head or director of an administrative unit which provides operational support (custodian) for information systems owned by another TAMUCC department shall have the responsibility for ensuring that an appropriate security program is in effect and that compliance with TAC standards is maintained for the supported information systems.

3.4 Operational responsibility for compliance with TAC standards may be delegated by the head of the administrative unit to the appropriate information system support personnel (e.g. system administrators) within the department.
3.5 Mission critical or confidential information maintained on an individual workstation or personal computer must be afforded the appropriate safeguards stated in the TAC standards. It is the responsibility of the operator, or owner, and/or departmental systems administrator of that workstation or personal computer to insure that adequate security measures are in place.

4. COMPLIANCE ASSESSMENT REPORTING

4.1 Administrative units having ownership or custodial responsibility for electronic information systems shall ensure that on an annual basis, a security assessment report is filed with the Office of the Assistant Vice President for Technology. The report shall be filed by the designated system administrator or custodian of the information system.

4.2 Administrative units having responsibility for information resources which store, transmit, or process mission critical or confidential information may assess their security posture and measure their compliance with the TAC Information Security Standards by using the appropriate software security system.

Contact for Interpretation: Assistant Vice President for Technology