1. GENERAL

Texas A&M-Corpus Christi University supports and encourages Internet and intranet use for the benefits such use provides to all users of information resources. University information resources are strategic assets of the State of Texas and thus must be managed as valuable state resources. This procedure is established to achieve the following:

(1) to ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources,

(2) to establish acceptable practices regarding the use of information resources,

(3) and to educate individuals who may use information resources with respect to their responsibilities associated with such use.

2. APPLICABILITY

This university procedure applies to all university information resources.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with Internet and Intranet usage. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

Please also refer to Procedure 29.01.03.C2.25 “Exceptions from Risk Mitigation Measures.”

The intended audience is all users of university information resources.

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 Definitions.

4. PROCEDURES
4.1. All Internet and Intranet usage by university students, faculty, and staff must adhere to federal and state laws as well as Texas A&M System and university policies, rules, and procedures.

4.2. In accordance with Texas Administrative Code Rule 202.75 Information Resources Security Safeguards the Information Resource Manager may authorize the logging, monitoring, review, and interruption of Internet and Intranet usage on university information resources to ensure compliance with applicable laws, policies, rules, and procedures or to monitor network performance and maintenance activities.

4.3. All Sensitive Information must be encrypted during transmission and storage.

4.4. Internet, Intranet, and email usage on information resources functioning as servers or storing Sensitive Information must be limited to business purposes only to minimize threats such as malware.

4.5. Resource custodians are required to ensure that all systems and software accessing the Internet and Intranet are up-to-date with security patches and the system’s protection software are maintained at the manufacturer’s current version and, if applicable, malware definitions.

4.6. Prior to initiating any education or research related to inappropriate Internet or Intranet content, as outlined in 4.1, faculty must notify the appropriate academic dean in writing. This written notification must contain a list of measures that shall be taken to protect non-project student, faculty, staff, and other personnel from exposure to the project information.

1. Course listings must identify the inclusion of this type of material.

2. Students attending these courses must be at least 18 years of age on the first day of class.

5. CONSEQUENCES FOR VIOLATIONS

All university employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this university procedure are subject to loss of access privileges to university information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of
this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.

Additional guidance may be found, but is not limited to, the following policies and rules.

- **Texas A&M System Policy**
  - 01.03 Appointing Power and Terms and Conditions of Employment
  - 07.01 Ethics Policy, TAMUS Employees
  - 32.02 Discipline and Dismissal of Employees
  - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  - 33 Employment, Standards of Conduct

- **Texas A&M University-Corpus Christi Rule**
  - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
  - 13.02.99.C1 Student Disciplinary Proceedings

Contact for Interpretation: Information Security Office

Office of Responsibility: Office of the Associate VP for Information Technology and CIO