

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.19 Security Training

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

Understanding the importance of information security, and individual responsibilities, and accountability pertaining to information security are paramount to achieving organization security goals. This can be accomplished with a combination of general information security awareness training and targeted, product-specific training. The security awareness and training information needs to be ongoing and updated as needed. The purpose of the security training procedure is to describe the requirements to ensure each user of university information resources receives adequate training on information security issues.

2. APPLICABILITY

This university procedure applies to all users of 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 security training. 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. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this university procedure based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual security assessment report (See University Rule 21.01.06.C2 Security of Electronic Information Resources).

3. DEFINITIONS

Please refer to University Procedure 21.01.06.C2.01 Definitions.

4. PROCEDURES

4.1. All university personnel are required to complete an Information Security Awareness training course that has been approved by the Information Resource Manager.

- (1) All employees are required to demonstrate a mastery of this training by completing a post training examination with a correct answer percentage set by the Information Resource Manager.

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- (2) All new employees shall complete this training prior to being assigned any university access credentials and accessing any university information resources.
 - (3) All university personnel are required to complete this training bi-annually.
 - 4.2. The Information Resources Manager may direct any university employee assigned administrative access to university information resources, such as resource custodians, are required to attend addition security awareness training provided by Media and Computer Services.
 - 4.3. Departments may assign their personnel additional security related training requirements.
 - 4.4. The Information Resource Manager shall oversee the preparation, maintenance, and distribution of one or more information security manuals that concisely describe how university rules and procedures relate to the security of university information resources and Sensitive Information.
 - 4.5. The Information Resource Manager shall oversee the development and continuation of an information security training program, in addition to the required Information Security Awareness training, that shall disseminate information related to the security of university information resources and Sensitive Information.
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

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 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: Assistant Vice President for Technology

Office of Responsibility: Executive Vice President, Finance & Administration