

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.18 Risk Assessment and Mitigation

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

Risk assessments are vital procedures for maintaining continuity of university operations, the security of information resources, and meeting the legal requirements for protecting confidential information. The purpose and goal of these assessments can only be achieved if the assessments are conducted effectively. The purpose of this university procedure is to implement a monitoring process which adequately provides management with assurance that the information on which risk assessment assertions are made is correct. The goal of these procedures is to assist Texas A&M University-Corpus Christi departments with improving the value and accuracy of their risk assessments and the effectiveness of their use of the Information Security Awareness, Assessment and Compliance (ISAAC) system.

2. APPLICABILITY

This university procedure applies to all information resources that are attached to the university network.

The intended audience includes all university personnel involved in performing, approving, or making risk management decisions related to information security risk assessments.

3. DEFINITIONS

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

4. PROCEDURES

4.1. Deans, division managers, and department heads shall not limit risk assessments to the risks associated with information resources.

- (1) Deans, division managers, and department heads shall regularly assess risks related to any area that might adversely affect the university (e.g. safety of personnel, management of sensitive information, training, business continuity, disaster recovery, etc).
- (2) Deans, division managers, and department heads are responsible for monitoring the mitigation of all risks associated with the risk assessments for which they are responsible.
- (3) Risk assessments are a collaborative process and should involve

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

representatives from different levels of the business unit conducting the assessment.

- 4.2. Resource custodians are required to conduct an annual risk assessment of all university information resources for which they have been assigned responsibility as per University Rule 21.01.06.C2 Security of Electronic Information Resources.
- 4.3. To reduce cost and centrally manage risks associated with university information resources, all resource custodians will utilize the ISAAC tool to conduct risk assessments.
- 4.4. Deans, division managers, and department heads are responsible for reviewing all ISAAC reports and accepting all risks associated with information resources that fall within their responsibility.
 - (1) Completed ISAAC reports, signed by the appropriate deans, division managers, and department heads, shall be submitted to the Information Resource Manager by no later than May 31st.
 - (2) Deans, division managers, and department heads are responsible for monitoring the mitigation of all risks associated with the information resources for which they are responsible.
- 4.5. The Information Resource Manager or representatives from this office will review all university ISAAC reports for unacceptable risk to university information resources and, to reduce costs associated with risk mitigation, identify issues and trends that can be globally addressed.
- 4.6. The Information Resource Manager may assign additional risks to any information resource or determine that any risk associated with any university information resource is unacceptable and require additional risk mitigation steps.
- 4.7. The Information Resource Manager will consolidate ISAAC information and present university executive management with a yearly report outlining the risks associated with the university's information resources by no later than August 30th.
- 4.8. Any changes associated with a university information resource must be preceded by a risk analysis of the ramifications to other university information resources. The Change Management Team (See University Procedure 21.01.06.C2.06 Change Management) will integrate risk assessment into the university's change management guidelines.
- 4.9. The Information Resource Manager or representatives from this office may conduct network and system detection, scanning, and monitoring to provide

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

confirmation and/or information regarding the configuration and classification (e.g., contains Sensitive Information) of a department's information resources.

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: Assistant Vice President for Technology

Office of Responsibility: Executive Vice President Finance & Administration