

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.23 System Development and Acquisition

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

The purpose of the system development and acquisition procedure is to describe the requirements for implementing application software that has been developed or acquired by authorized Texas A&M University-Corpus Christi personnel.

2. APPLICABILITY

This university procedure applies to university information resources that store or process mission critical and/or confidential information.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with system development and acquisition. 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).

The intended audience is university owners and custodians that manage university information resources that store or process Sensitive Information.

3. DEFINITIONS

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

4. PROCEDURES

4.1. Media and Computer Services, in conjunction with the department information resource owners, or their designees, are responsible for developing, maintaining, and participating in a System Development Life Cycle for all university system and software development projects. All software developed in-house which runs on production systems must be developed according to the System Development Life Cycle. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

testing; implementation; and post-implementation maintenance and review. This methodology ensures that the system deployments and developed software shall be adequately documented and tested before it is used for critical university information.

- 4.2. All production systems must have designated information resource owners and custodians for the critical information they process. Owners, and/or their designees, must perform periodic risk assessments of production systems to determine whether the controls employed are adequate.
- 4.3. All system and software acquisitions must follow the procedures defined in University Procedure 21.01.06.C2. 22 Software Licensing. The Information Resource Manager may consolidate or disapprove any system or software purchase based on risk assessment, existing licensing agreements, or consolidation of university resources.
- 4.4. Where resources permit, there shall be a separation between the production, development, and test environments. This ensures that security is rigorously maintained for the production systems, while the development and test environments can maximize productivity with fewer administrative restrictions.
- 4.5. All production systems must have an access and authorization control system that restricts system access and limits the privileges available to each user. Each production system must have an assigned information resource custodian.
- 4.6. Implementation and usage of systems and software must be reviewed annually.

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

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 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