

**UNIVERSITY PROCEDURES**  
**TEXAS A&M UNIVERSITY-CORPUS CHRISTI**

---

**21.01.06.C2.06 Change Management**

*Approved June 11, 2007*

*Supplements University Rule 21.01.06.C2*

1. GENERAL

The Information Resources infrastructure at Texas A&M University-Corpus Christi is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between information resources infrastructure grows, the need for a strong change management process is essential.

From time to time each information resource element requires an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these and other changes is a critical part of providing a robust and valuable information resources infrastructure. A well-structured, documented, and enforced Change Management program will positively affect management, accountability, business continuity, distribution of resources, and security within the university's broad and rich technological environment.

2. APPLICABILITY

This university procedure applies to all university information resources and all individuals that install, operate, or maintain information resources connected to the university network.

The purpose of the implementation of this university procedure is to provide a set of measures that will mitigate information security risks associated with change management. 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

**UNIVERSITY PROCEDURES**  
**TEXAS A&M UNIVERSITY-CORPUS CHRISTI**

---

4. PROCEDURES

- 4.1. The Information Resource Manager, with consultation from the University Technology Council, shall form a Change Management Team to facilitate and improve management, accountability, business continuity, distribution of resources, security within the university's evolutionary network, and information resources.
- (1) The Change Management Team shall be formed from key information resource custodians and department managers from throughout the university.
  - (2) The Information Resource Manager or representatives from this office shall work as members of this team.
  - (3) The Information Resource Manager or representatives from this office shall be responsible for providing the University Technology Council with periodic reports as to the team's activities, progress, successes, and challenges.
  - (4) Other university departments and colleges with information resources that are connected to the university network shall provide representatives to the team.
  - (5) Because of the potential for the discussion of Sensitive Information these team meetings may be closed to non-team members at the discretion of the Change Management Team.
- 4.2. The Change Management Team shall develop, publish, maintain, and enforce a set of university-wide change management guidelines.
- (1) The guidelines shall outline the team's processes for managing change within the university's network environment and information resources to include the approval and disapproval of change requests.
  - (2) The guidelines shall outline the procedures for submitting scheduled and unscheduled change requests.
  - (3) The guidelines shall outline the procedures for maintaining a change management log detailing, at least, the time and date, information resources, resource custodians, nature of change, and detailed notes pertaining to all change requests.
  - (4) Disapproval of change requests may be appealed to the University Technology Council who will provide a final ruling on the matter.

## **UNIVERSITY PROCEDURES**

### **TEXAS A&M UNIVERSITY-CORPUS CHRISTI**

---

- 4.3. The Change Management Team is responsible for reviewing all changes pertaining to information resources connected to the university network.

Examples of such changes include, but are not limited to the change, update, modification, addition, or removal of network devices, business related servers, business related applications (i.e. web servers, databases), systems containing Sensitive Information, etc. Specifics shall be outlined in the change management guidelines.

- 4.4. All university information resources must comply with the findings of the Change Management Team and its documented change management guidelines.

- 4.5. Departments and colleges that maintain information resources and networks connected to the university network shall form an departmental change management team to manage change within their environment. Any changes that will affect the university network or information resources must still be presented to and approved by the Change Management Team prior to the implementation of the change.

- 4.6. All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) must be reported to or coordinated with the Change Management Team prior to the event and with sufficient lead time, when available, to notify the resource custodians of affected information resources.

- 4.7. Changes due to emergency situations that do not provide enough time to contact the Change Management Team shall be addressed at the earliest opportunity.

#### **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.

**UNIVERSITY PROCEDURES**  
**TEXAS A&M UNIVERSITY-CORPUS CHRISTI**

---

- 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