



TEXAS SOUTHERN UNIVERSITY
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology
AREA: Information Security

Policy 04.06.08

SUBJECT: Change Management Policy

I. PURPOSE

The purpose of the Change Management Policy is to manage changes in information technology in a rational and predictable manner so that staff can plan accordingly. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy.

II. SCOPE

The Information Resource infrastructure at TSU is continuously expanding and 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 the information technology infrastructure grows, the need for a strong change management process is essential. From time to time, each information technology 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 changes is a critical part of providing a robust and valuable information technology infrastructure.

III. OWNERSHIP AND RESPONSIBILITIES

The Change Management Policy applies to all individuals who install, operate or maintain information resources and technology, including but not limited to faculty, staff, students, and consultants, and vendors.

IV. CHANGE MANAGEMENT POLICY

- A. Every change to a TSU information resource and technology, such as operating systems, computing hardware, networks, and applications is subject to this Change Management Policy. All changes must follow change management procedure, including registering equipment, software and IT processes with OIT for approval. All changes affecting computing environmental facilities (e.g. air-conditioning, water, heat, plumbing, electricity, and alarms) should be reported to or coordinated with the leader of the

change management process. A formal written change request must be submitted for all changes, both scheduled and unscheduled. All scheduled change requests must be submitted in accordance with change management procedures as determined by the Information Resource Manager, so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request. Each scheduled change request must receive formal Change Management Committee approval before proceeding with the change. The Change Management is determined by the Information Resource Manager.

- B. The appointed leader of the Change Management Committee and/or Information Security Officer may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or adequate resources are not readily available. Adequate resources may be a problem on weekends, holidays or during special events.
- C. Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the change management procedures. A change review must be completed for each change, whether scheduled or unscheduled and whether successful or not.

V. CHANGE MANAGEMENT LOG

A change management log must be maintained for all changes. The log must contain, but is not limited to:

- A. Date of submission and date of change;
- B. Owner and custodian contract information;
- C. Nature of the change; and
- D. Indication of success or failure.

All University information systems must comply with an Information Resources change management process that meets the standards outlined above.

VI. DISCIPLINARY ACTION

Violation of this policy may result in immediate Disciplinary Action pursuant to University policy (MAPP 02.05.03 – Discipline and Termination Policy).

VII. APPLICABLE TSU SECURITY POLICY STANDARDS

All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy – MAPP 04.06.22). Applicable security standards include, but are not limited to:

- Security Standard 12
- Security Standard 14
- Security Standard 15

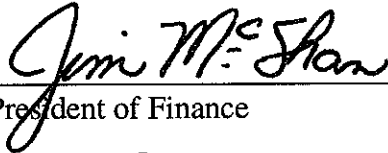
VIII. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer

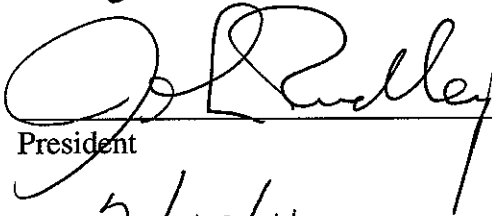


Review: Every year, on or before September 1

IX. APPROVAL



Vice President of Finance



President

2/18/11

Effective Date