Introduction

The Information Resources (IR) infrastructure at UTMB is continuously expanding and becoming more complex. As the interdependency between the users and IR infrastructure grows, the need for a strong change management process is essential.

From time to time each IR 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 IR infrastructure.

Purpose

The purpose of the Change Management Practice Standard is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of IR.

Audience

The UTMB Change Management Practice Standard applies to all individuals that install, operate or maintain IR.

Glossary

- Production system – A stable environment that is used to conduct or support UTMB business and that is secured to prevent any development or prevent any unauthorized changes.
- Development system – An environment where developers are making changes to code, files, and/or setup. This environment may or may not mimic the production environment.
- Test system - An environment that mimics the production system and that is secured to prevent any development or change. The test system is where changes are tested by users before they are moved to production.

Practice Standards

- Every significant change to UTMB multi-user, production IR including operating systems, computing hardware, networks, and applications is subject to this Change Management Practice Standard.
Change Management, continued

Practice Standards

- All multi-user computer and communications systems used for production processing at UTMB must employ a formal change management procedure which is used to ensure that only authorized changes are made. The change management procedure must be used for all significant changes to software, hardware, communications networks, and related procedures. The change management procedure must also be used for changes made by third parties (i.e., vendors) and for changes affecting computing environmental facilities (e.g., airconditioning, water, heat, plumbing, electricity, and alarms).

- The change management procedure must address: 1) formally identifying, classifying, prioritizing and requesting changes; 2) identifying and deploying emergency changes; 3) assessing potential impacts of changes; 4) authorizing changes and exceptions; 5) testing changes; 6) change implementation and backout planning; and 7) documenting and tracking changes.

- A formal change request must be submitted to the change management committee for all significant changes, both scheduled and unscheduled.

- Each change, scheduled or unscheduled, must be reviewed by the system owner or assigned agent(s) prior to the submission to change management committee.

- Each scheduled and unscheduled change request must receive formal approval from the change management committee before proceeding with the change.

- All changes must be properly communicated to affected parties prior to change implementation to ensure that implementation reasonably minimizes potential business disruptions.

- A change management log must be maintained for all changes. The log must contain, but is not limited to:
  o date of submission and date of change
  o owner and custodian contact information
  o nature of the change and potential impact of the change
  o indication of success or failure

- All new or modified programs must be tested and approved by the appropriate user and either Information Services supervisors (if the program is centrally managed) or departmental supervisors (if the program is managed by a department or school)
Change Management, continued

- All new or modified programs will be tested in a separate test environment (either logically or physically separate) where possible. Exceptions should be documented in the change request.
- Copies of production data shall not be used for testing unless the data has been declassified or unless all persons involved in testing are authorized by the data owner to access the production data.
- Approval documentation associated with each change must be retained for a period of three years to maintain necessary audit trails. Testing documentation, including test plans and test results supporting each change, must be retained for a period of one year.
- All UTMB information systems must comply with an IR change management process that meets the standards as outlined above.
- If applicable, change requests must specify how long production data will remain in a test system following a successful system upgrade. Production data should not remain in a test system for longer than 90 days following a successful system upgrade.

Disciplinary Actions

Violations of this policy may result in disciplinary action which may include termination for employees; a termination of employment relations in the case of contractors or consultants; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTMB IR access privileges, civil and/or criminal prosecution.

References
- UTMB Acceptable Use of Information Resources Policy
- UTMB Information Resources Security Policy
- UTMB IR Security Glossary
- UTMB IT Security Procedures – Change Management
- Texas Administrative Code 1 TAC §§202 - Information Security Standards
- UT System UTS 165 – Information Resource Security