IR Security Policy Approval Process

Introduction

The UTMB Information Security Policy Principles are the foundation for the Information Security Program. These principles have been developed by interpreting HIPAA, Texas Administrative Code 1 TAC §§202 (Information Security Standards) and other legislation and legal requirements, understanding University business needs, evaluating existing technical implementations, and by considering the cultural environment.

Changing Environment

The business, technical, cultural, and legal environment of UTMB, as it relates to information technology use and security, is constantly changing. The Security Policy Principles will be revised as required to comply with changes in law or administrative rules or to enhance its effectiveness.

Technology Neutral

These Policy Principles are technology neutral and apply to all aspects of information technology. However, it is possible that emerging technologies or new legislation could impact these principles in the future.

Ownership

The Security Policy Principles are owned by the UTMB Information Resources Manager (IRM).

Approval Process

The approval process is outlined in Policy 2.1.2 of the UTMB Institutional Handbook of Operating Procedures (IHOP).
IR Security Policy Approval Process, *Continued*

**Change Drivers**

A number of factors could result in the need or desire to change the Security Policy Principles. These factors include, but are not limited to:

- Review schedule
- New legislation
- New technology
- Audit report
- Business requirements
- Cost/benefit analysis
- Cultural change

**Change Process**

Updates to the UTMB Information Security Policy Principles, which include establishing new policy principles, modifying existing policy principles, or removing policy principles, can result from two different processes:

- Bi-annually, to correspond with the end of a legislative session, the IRM, or designee, will review the Policy Principles for possible addition, revision, or deletion. An addition, revision, or deletion is created if it is deemed appropriate.

- Any user may propose the establishment, revision, or deletion of any policy principle at any time. These proposals should be directed to the Information Security Officer (ISO) who will evaluate the proposal and make recommendations to the IRM.

Once a change to the Security Policy Principles has been approved by the IRM it will be submitted to the process defined in IHOP Policy 2.1.2.
IR Security Policy Approval Process, *Continued*

**Change**
**Distribution and Notification**

Once a change to the Security Policy Principles has been approved according to the IHOP Policy 2.1.2 process, the following steps must be taken to properly document and communicate the change:

- The appropriate IHOP web pages will be updated with the change.
- The UTMB Information Resources Security Manual will be updated with the change.
- The UTMB Information Resources Security Manual will be redistributed as appropriate.
- Training and compliance materials will be updated to reflect the change.
- The changes will be communicated using standard UTMB communications methods such as: internal cable TV system, UTMB daily announcements, iUTMB web page, newsletters, and communications meetings.

**Exceptions**

The UTMB Security Policy Principles set the security strategy for UTMB at a very high level and are technology neutral. As such, there is no need for an exception process for the Security Policy Principles.
IR Security Policy Approval Process, Continued

Policy Principles
Change Request

1. Change trigger
2. Appoint sponsor
   Establish time line
   Draft Proposal
3. Review proposal
4. Accept Proposal?
   Yes
   Stakeholder Review
   Modification required?
   No
   Final approval by IRM
   Proposal Accepted for IHOP?
   Yes
   Publish and Communicate
   Stop
5. No
   Make modifications
   Yes
   Notify originator
   Stop

July 12, 2001