IR Security Management Practice Standards Approval Process

**Introduction**
The UTMB Information Security Practice Standards provide the operational detail required for the successful implementation of the Information Security program. These security practice standards were developed based on and cross-referenced to the Security Policy Principles which can be found in the UTMB Institutional Handbook of Operating Procedures (IHOP). In addition these standards have been developed by interpreting HIPAA, Texas Administrative Code 1 TAC §§202 (Information Security Standards) and other legislation and legal requirements, understanding 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 Practice Standards will be revised as needed to comply with changes in law or administrative rules or to enhance its effectiveness.

**Technology Neutral**
These Practice Standards are technology neutral and apply to all aspects of information technology. However, emerging technologies or new legislation will impact these Practice Standards over time.

**Ownership and Approval**
The Security Practice Standards are owned by the UTMB Information Resources Manager (IRM). The IRM, or designee, is the only authority that can approve modifications to the Security Practice Standards.
IR Security Management Practice Standards Approval Process, Continued

Change Drivers
A number of factors could result in the need or desire to change the Security Practice Standards. These factors include, but are not limited to:

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

Change Process
Updates to the UTMB Information Security Practice Standards, which include establishing new practice standards, modifying existing practice standards, or removing practice standards, can result from three different processes:

- At least annually, the Information Security Officer (ISO), or designee, will review the Practice Standards for possible addition, revision, or deletion. An addition, revision, or deletion is created if it is deemed appropriate.

- Every time new Information Resources (IR) technology is introduced into UTMB a security assessment must be completed. The result of the security assessment could necessitate changes to the Security Practice Standards before the new technology is permitted for use at UTMB.

- Any user may propose the establishment, revision, or deletion of any practice standard at any time. These proposals should be directed to the ISO who will evaluate the proposal and make recommendations to the IRM. Significant proposed changes should also be presented to the Computing Standards Advisory Group (CSAG) for comment.
IR Security Management Practice Standards Approval Process, Continued

**Change Distribution and Notification**

Once a change to the Security Practice Standards has been approved by the IRM, or designee, the following steps will be taken as appropriate to properly document and communicate the change:

- The appropriate IR Security web pages will be updated with the change.
- 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.

**Exception Introduction**

The UTMB Security Practice Standards provide the techniques and methodology to protect UTMB IR assets. While these Practice Standards are technology independent they are more closely linked to the technology than the Policy Principles and are hence more likely to be impacted by changing technology, legislation, and business requirements.

An exception is a method used to document variations from the rules. Example are:

- Allowing a desktop modem when the Practice Standard states desktop modems are not permitted.
- Giving an individual elevated privileges in comparison to another individual with similar responsibilities.
IR Security Management Practice Standards Approval Process, Continued

Exception Process

The steps for permitting and documenting an exception are:

- A request for an exception is received by the ISO along with a business case for justifying the exception.
- The ISO analyzes the request and the business case and determines if the exception should be accepted, denied, or if it requires more investigation.
- If more investigation is required the ISO and IR technical staff determine if there is a cost effective solution to the problem that does not require an exception.
- If there is not an alternate cost effective solution, and the risk and/or administrative overhead is minimal, the exception may be granted.
- Each exception must be re-examined according to its assigned schedule. The schedule can vary from three months to 12 months depending on the nature of the exception.
- Any exception request that is rejected may be appealed to the IRM.
IR Security Management Practice Standards Approval Process, *Continued*

**Practice Standards Change Process**

1. **Change trigger**
2. **Appoint sponsor**
   - Establish time line
   - Draft Proposal
3. **Review proposal**
4. **Accept Proposal?**
   - Yes
   - Make modifications
     - **Stakeholder Review**
6. **Modification required?**
   - No
   - **Final approval by IRM or delegate.**
   - **Proposal Accepted by the IRM or delegate?**
     - Yes
     - **Publish and Communicate**
     - **Stop**
   - **Stop**

   - No
     - Notify originator
     - **Stop**

July 12, 2001
IR Security Management Practice Standards Approval Process, *Continued*

**Practice Standards Exception Process**

- **Start Exception Process**
  - Exception request and business case submitted to ISO
  - Regular review of an exception
  - ISO analysis request and business case
  - ISO Accepts exception request?
    - Yes
      - ISO Accepts exception request?
        - No
          - Not outright
            - ISO and IR technical team assess request.
        - Yes
          - Document exception and notify requestor
    - No
      - Document rejection and notify requestor
      - End Exception Process

*July 19, 2001*