Remote Access

Introduction
The use of high speed cable and DSL services, web-based applications, as well as improved wireless (Wi-Fi) network technology have made the remote access of UTMB Information Resources (IR) a very straightforward and simple process. When accessing UTMB IR remotely, university, state and federal policy and regulatory statutes require certain administrative, technical and physical security controls to be in place, verified and reported on.

Purpose
The purpose of the UTMB Remote Access Practice Standard is to provide requirements and guidelines to support the accessing of UTMB’s information resources from remote locations in accordance with established policy, regulatory requirements and best practices.

Audience
The UTMB Remote Access Practice Standard applies to all individuals who may be required to connect to and conduct normal business functions from remote locations.

Implications
- All policies and practice standards applying to on-site “hardwired” or wireless IR and the users of on-site IR apply to remotely connected IR and users.
- Remote locations include any place that a UTMB controlled first point of network contact cannot be established. These may include private homes, associated business locations and public access points.
- Remote access methods may include dial-up lines, high-speed cable or DSL, site-to-site internet tunnel, leased line, or publicly accessible Wi-Fi access points.
- Time duration limits on active and inactive connections will be enforced.
Privacy

Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of UTMB are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 1 TAC §§202 (Information Security Standards), Information Resource Standards and in the University of Texas System, UTS 165 - Information Resources Use and Security Policy.

Confidential Digital Data Management

Confidential Digital Data includes social security numbers, Protected Health Information (PHI), Confidential Research Data, digital data associated with an individual and/or digital Data protected by law. Confidential digital data must be secured and protected while at rest on mobile computing/storage devices, i.e., portable hard drives, removable media, laptops, PDA or flash drive) and in transit (via the Internet or non-trusted network).

Practice Standard

- Anyone requiring remote access to the UTMB network is required to sign a non-disclosure agreement prior to being granted access.
- A UTMB domain users account is required for VPN access to UTMB resources. Accounts will be used to access UTMB resources only by the persons to whom it was assigned.
- Remote access is provided to specific UTMB resources for UTMB related business functions. Additionally, Internet access via remote connection from UTMB networks is supported. All applicable policy and practice standards, including appropriate and incidental use practice standards apply to all accesses via remote connection to UTMB.
- UTMB IR users may only access the UTMB network through an institutionally established dedicated circuit, VPN or modem pool. Direct IR access methods (modem lines on individual IR systems) must be approved by IS and disconnected when not in use.
  - As a condition of gaining access to UTMB’s network, remote users must secure their own connected systems in a manner consistent with UTMB’s requirements.
Remote Access, Continued

Practice Standards (cont)

- Remote users must maintain physical access controls, such as using screensaver to prevent incidental viewing by non-UTMB personnel, to ensure that only authorized users and appropriate uses of IR occur while remotely connected to UTMB networks.

- UTMB information will not be maintained (long-term storage or operation use, except as established by business agreements) on non-UTMB owned remote systems. Temporary or transitory maintenance of UTMB information on employee owned (laptop or home computer) is permitted, assuming all related security controls (password access, physical security, backups, etc.) are in place.

- Remote users must report all security incidents directly to the Computer Incident Response Team (CIRT) at (409) 772-3838 or cirt@utmb.edu.

- Web-based collaboration/file-sharing applications, such as “Webex”, can provide viewing and limited access to local resources during an active session. When using these application, the following security issues should be given strong consideration:
  
  - Sessions should be started no sooner than 15 minutes prior to collaboration or meeting time, and sessions should be closed immediately following the collaboration or meeting.
  
  - Unnecessary applications, services and network shares should be closed, discontinued or disconnected prior to starting a session.
  
  - When hosting a session, make use of available security features such as private sessions, passwords to join sessions and, when available, SSL (port 443) connections.
  
  - When participating in a session, understand the roles (owner, presenter, participant) and accesses these roles provide. Always require a user prompt (challenge/request) change roles or establish access to local resources.
Vendor Access, Continued

**Disciplinary Actions**
Violation 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 Email Use Policy
- UTMB Internet Use Policy
- UTMB IR Security Management Practice Standards Approval Process
- UTMB IR Security Glossary
- UTMB IR Security Monitoring Practice Standard
- UTMB IR Password Management Practice Standard
- UTMB IR Account Management Practice Standard
- UTMB IR Special Access Practice Standard