Network Access

Introduction

The UTMB network infrastructure is provided as a central utility for all users of UTMB Information Resources. It is important that the infrastructure, which includes cabling and the associated ‘active equipment’, continues to develop with sufficient flexibility to meet UTMB demands while remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the UTMB Network Access Practice Standard is to establish the rules for the access and use of the network infrastructure. This includes issues of documentation and change control, as well as those of connectivity to other networks such as the Internet and extranets. These rules are necessary to preserve the integrity, availability, and confidentiality of UTMB information.

Audience

The UTMB Network Access Practice Standards apply equally to all individuals with access to any UTMB Information Resource (IR).

Implications

- Configurations and set-up parameters on all hosts attached to the UTMB network must comply with UTMB IR Security Management Practice Standards.
- Prior to being permitted to use computers connected to the UTMB network, all users must have their identity verified with a User ID and secret password (or by other means which provide equal or greater security); and are accountable for activities associated with such use.
- UTMB reserves the right to audit the security measures in effect on these connected systems without prior warning.
- UTMB reserves the right to immediately terminate network connections with systems not meeting such requirements.
Network Access, continued

Sensitive Digital Data Management

- Users are permitted to use only network addresses issued to them by UTMB IS.
- All remote access to UTMB will be either an approved modem pool or via an Internet Service Provider (ISP) using UTMB approved protocols.
- Devices attached to the UTMB data network cannot have a modem.
- Users must not extend or re-transmit network services (i.e., DNS, DHCP, dynamic routing, etc.) in any way. This means users must not install a router, switch, hub, or wireless access point to the UTMB network without Information Services (IS) Network and Security Services (NSS) approval or assistance.
- Users are not permitted to alter network hardware or software that provides network services without IS NSS approval.
- Computer systems requiring network connectivity that are not owned or supported by UTMB must conform to IS NSS standards and IR Security Management Practice Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, UTMB users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the UTMB network infrastructure.
- All network components, including data closets, wiring and fiber, routers, switches, concentrators, and hubs, must be protected from unauthorized access.
- Firewalls and other enterprise network security measures must be implemented to provide appropriate network security.
Network Access, continued

Practice Standards (con’t)

- Multiple simultaneous on-line sessions are not permitted (i.e., one User ID equals one log-in session).
- Computer Systems requiring network connectivity must use the following approved System Identification/Logon Banner: “The information system you are using is the property of or licensed to UTMB. For the integrity of the system and to comply with state and federal mandates, policy and practice standards govern its use. Please understand that there is no privacy in your use of this digital information system. For security and other reasons related to UTMB operations, activities on these systems are monitored and may be recorded by systems support personnel. Anyone using a UTMB information system consents to such monitoring. Pursuant to the Texas Administrative Code (Title I, Part 10, §§202), all UTMB information systems are solely for the use of authorized users. UTMB management or the appropriate law enforcement agency may be advised and be provided evidence of any individual using a UTMB information system without authority, in an unauthorized manner, for inappropriate activity, or to violate the law. Prior to accessing this information system you should be thoroughly familiar with UTMB’s policies and practice standards, accessible at http://www.utmb.edu/policy/is/listing.htm. By using this information system, you acknowledge that you understand these issues and will comply with these policies.”
- Connection to the UTMB network implies acceptance of the terms and conditions set forth in applicable IR Security Policies and Practice Standards.

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