Network Configuration

Introduction
The UTMB network infrastructure is a vital information asset 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 such as routers and switches, continues to develop with sufficient flexibility to meet user demands while remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhances user services.

Purpose
The purpose of the UTMB Network Configuration Security Practice Standard is to establish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of UTMB information.

Audience
The UTMB Network Configuration Practice Standard applies to all individuals with access to any UTMB Information Resources (IR).

Implications
- The UTMB network infrastructure must be configured such that it can prevent and/or detect attempts to connect unauthorized computer devices.
- Configuration and set-up parameters on all hosts and workstations attached to the UTMB network must comply with UTMB IR Security policies and practice standards.

Sensitive Digital Data Management
Sensitive Digital Data, as defined by UTS 165, includes social security numbers, Protected Health Information (PHI), Sensitive Research Data, digital Data associated with an individual and/or digital Data protected by law. Sensitive digital Data must be secured and protected while at rest (electronic storage on a hard drive, digital or optical media), mobile (laptop, PDA or flash drive) and in transit (via email or the Internet).
Network Configuration, continued

**Practice Standards**

- Users must not extend or re-transmit network services in any way. This means users must not install a router, switch, hub, or wireless access point to the UTMB network without UTMB IS Network and Security Services approval.
- Users must not install network hardware or software that provides network services without UTMB IS Network and Security Services approval.
- Users are not permitted to alter network hardware in any way.
- UTMB Information Services owns and is responsible for the UTMB network infrastructures and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent UTMB network infrastructure capable of exploiting new network developments, all cabling must be installed by UTMB IS Network and Security Services or an approved contractor.
- All network connected equipment must be configured to a specification approved by UTMB IS Network and Security Services.
- All hardware connected to the UTMB network is subject to UTMB IS Network and Security Services standards for management and monitoring.
- Changes to the configuration of active network management devices must not be made without the approval of UTMB IS Network and Security Services.
- The UTMB network infrastructure supports a well-defined set of approved networking protocols (primarily TCP/IP and IPX, with some AppleTalk). Any use of non-sanctioned protocols must be approved by UTMB IS Network and Security Services. The networking addresses for the supported protocols are allocated, registered and managed centrally by UTMB IS.
- All connections of the campus network infrastructure to external third party networks are the responsibility of UTMB IS Network and Security Services, including connection to external telephone networks.
- UTMB IS firewalls must be configured and maintained as per the UTMB IR Firewall Management procedures.
- The use of departmental firewalls is not permitted without the written authorization from the UTMB IRM.
Network Configuration, continued

Disciplinary Actions

Violations of these security practice standards 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 IR Server Hardening Practice Standard
- UTMB IR Network Access Practice Standard
- UTMB IR Firewall Management Procedures