Platform Hardening

Introduction
Platforms are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the platforms are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

Purpose
This document describes the requirements for installing a new platform or upgrading an existing platform in a secure fashion and maintaining the security integrity of the platform and application software to ensure that information systems equipment continues to operate as it should, thus supporting UTMB in achieving its mission.

Audience
The UTMB Platform Hardening Practice Standard applies to all individuals that are responsible for the installation of new Information Resources (IR), the operations of existing IR, and individuals charged with IR Security.

Implications
- Before connecting to the UTMB network, all platforms must be preauthorized by appropriate management (i.e., accreditation).
- New platforms connected to the data network and existing systems that are upgraded must have the preventative maintenance performed before the platforms are put into production. This includes such issues as removing default passwords, adding vendor patches, and removal of application software that may be included in a default installation, but is not necessary or wanted as part of the system’s operational capacity.
- To remain connected to the UTMB network, all platforms must comply with applicable baseline IR security policies and practice standards (i.e., certification).
- Information must be protected in a manner commensurate with its confidentiality, sensitivity, value, and criticality.
Sensitivity Digital Data Management

Sensitive Digital Data, as defined by UTMB 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).

Practice Standards

- A platform must not be connected to the UTMB network until it is in a certified secure state and the network connection is approved by Information Services (IS Network and Security Services (NSS)).
- Security patches must be implemented within the timeframe specified from IS.
- After a reasonable delay for the stabilization of the new release, the most recent version must be used in order to take advantage of recent security improvements.
- The Platform Hardening Procedure provides the detailed information required to harden a platform and must be implemented for certification. Some of the general steps included in the Platform Hardening Procedures include:
  - Installing the operating system from an IS approved source
  - Applying vendor supplied patches
  - Removing unnecessary software, system services, and drivers
  - Setting security parameters, file protections and enabling audit logging
  - Disabling or changing the password of default accounts
- IS will monitor information security vulnerability advisories issued by trusted organizations such as SANS or CERT.
- IS will monitor security issues, both internal to UTMB and externally, and to the extent possible, will centrally manage the release of security patched on behalf of UTMB.
- IS will test security patches against IS core resources before release where practical.
- IS may make hardware resources available for testing security patches in the case of special applications.
Network Configuration, continued

**Practice Standards (con’t)**

- Platforms must run only necessary services. After it has been determined what services are needed, all unnecessary services should be shut down.
- The platform must have all default account passwords changed and after determining what default accounts are required, have all other default accounts disabled.
- The platform may not function as a relay for SMTP or other means of relaying non-UTMB related email.
- Servers must authenticate all users to ensure authorized access to the resource.
- All platforms connected to the UTMB network must comply with applicable IR Security policy and practice standards.

**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 Network Access Practice Standard
- UTMB IR Platform Hardening Procedures