Password Management

Introduction
User authentication is a means to control who has access to an automated Information Resource system. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to UTMB.

Three factors, or a combination of these factors, can be used to authenticate a user. Examples are:

- **Something you know** – password, personal identification number (PIN)
- **Something you have** – token (i.e., SmartCard)
- **Something you are** – biometrics (fingerprint, iris scan, voice recognition)
- **A combination of factors** – token (i.e., SmartCard) and a PIN

Purpose
The purpose of the UTMB Password Management Practice Standard is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of UTMB user authentication mechanisms and to identify the measures that users are expected to take in ensuring the security of their account and UTMB IR.

Audience
The UTMB Incident Management Practice Standard applies equally to all individuals who use any UTMB IR.

Implications
- Computer and communications system access control must be achieved via passwords that are unique to each individual user in compliance with UTMB security management policies and practice standards.
- All users must have their identity verified with a User ID and a secret password (or by other means which provide equal or greater security) prior to being permitted to use UTMB computers connected to its network.
- Users are responsible for all activity performed with their personal User ID. Similarly, users are prohibited from performing any activity with IDs belonging to other users.
- Passwords are the first level of protection from a would-be intruder. Once into the system, a knowledgeable user could do considerable damage. Thus, as a member of the user community, it is the responsibility of all users to choose a good password.
Password Management, continued

Sensitive Digital Data Management

UTMB Information Resource users are required to protect “Sensitive Digital Data” in accordance with UTMB Practice Standard 1.2.10 – Managing Sensitive Digital Data.

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).

Practice Standards

- User account passwords must not be disclosed to anyone. UTMB IS and its agents will not ask for user account passwords.
- Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software without the approval of the UTMB ISO. A procedure must be available to change the passwords.
- IS Help Desk password change procedures must include the following:
  - authenticate the user to the Help Desk before changing password
  - change to a strong password
  - the user must change password at first login
- All passwords, including initial passwords, must be constructed and implemented according to the following UTMB IR rules:
  - it must be routinely changed (every 180 days for normative use, every 30 days for administrative and special access privileges)
  - it must adhere to a minimum length of eight characters
  - it must be a combination of alpha and numeric characters
  - it must not be anything easily identified with the account owner such as: user name, social security number, nickname, relative’s names, birth date
  - it must not be recurring passwords created by combining a set of characters that do not change with a set of characters that predictably change (i.e., May2002, Jun2002, Jul2002, etc.)
  - it must not be dictionary words, acronyms, or common character sequences (i.e., 123456, qwerty, zxcvbn, etc.)
Password Management, continued

Practice Standards (con’t)

- A password history must be kept to prevent the frequent reuse of a password (minimally contains the last 20 passwords for each User ID)
- After ten (10) unsuccessful attempts to enter a password, the involved User ID must be suspended for thirty (30) minutes or until an administrator unlocks the User ID

- Generic accounts (used for service or email accounts) must have a minimum ten character password that includes alpha, numeric AND special characters.
- The display and printing of passwords must be suppressed such that unauthorized parties will not be able to observe or subsequently recover them.
- Stored passwords must be encrypted.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with UTMB.
- If the security of a password is in doubt, the password must be changed immediately.
- System administrators must not circumvent the Password Management Practice Standard for the sake of ease of use.
- In the event passwords are found or discovered, the following steps must be taken:
  - Take control of the passwords and protect them
  - Report the discovery to the UTMB IS Help Desk
  - Transfer the passwords to an authorized person as directed by the UTMB ISO
- Developers are prohibited from building or deploying ‘backdoor’ User ID’s or passwords which have special privileges and circumvent normal system access.
- All vendor supplied/default passwords must be changed before any computer or communications system is connected to the UTMB network.
- System Administrators, technical services staff and Service Desk will monitor and review Active Directory and system logs for suspicious and potentially malicious login activity (including excessive login attempts, account lockouts, etc.). Any evidence of confirmed malicious activity will be forwarded to CIRT. All records will be associated with the CIRT incident ticket and retained for a minimum of three (3) years (or six (6) years if ePHI involvement is confirmed).
Password Management, continued

Disciplinary Actions

Violations of this practice standard 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 Security Management Practice Standards Approval Process
- UTMB IR Security Procedures – Password Creation and Change
- UTMB IR Security Procedures – Password Escrow