**Account Management**

**Introduction**

Computer accounts are the means used to grant access to UTMB Information Resources (IR). These accounts establish accountability for IR usage. This means that creating, controlling and monitoring all computer accounts is extremely important to an overall security program.

**Purpose**

The purpose of the UTMB Account Management Practice Standard is to establish the rules for the creation, monitoring, control, and removal of user accounts.

**Audience**

The UTMB Account Management Practice Standard applies equally to all individuals with authorized access to any UTMB Information Resources.

**Implications**

- The computer and communications system privileges of all users, systems, and programs must be restricted based upon the concept of ‘minimum necessary’ use (i.e., users receive only those access privileges minimally required to perform their assigned job duties).
- User IDs may be granted to specific users only when approved in advance by recognized parties (i.e., ‘trusted requestors’) within the business function. Prior to being granted to users, application system privileges must be authorized by the involved owner.
- Computer and communications system privileges must be granted only by a clear chain of authority delegation.
- The computers and computer accounts given to users are to assist them in the performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive.

**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).
Account Management, continued

Practice Standards

- All accounts created must have an associated request and approval that is appropriate for the UTMB system or service.
- All users must sign the UTMB Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- All accounts must be uniquely identifiable using the assigned user name.
- No two people may ever have the same User ID throughout the lifetime of the system (i.e., User ID’s are not to be reused).
- All default passwords for accounts must be constructed in accordance with the UTMB Password Management Practice Standard.
- All accounts must have a password expiration that complies with the UTMB Password Management Practice Standard.
- All new user accounts that have not been accessed within 30 days will be disabled.
- All user accounts utilized by UTMB employees and students that have not been accessed within 90 days (due to inactivity) will be disabled. (Note: The inactivity period for non-UTMB personnel is 30 days.)
- All disabled accounts will be permanently deleted after 30 days of revocation.
- System Administrators:
  - are responsible for removing the accounts of individuals who change roles within UTMB or are separated from their relationship with UTMB
  - must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes
  - must have a formal process for periodically reviewing existing accounts for validity
  - are subject to independent audit review
  - must provide a list of accounts for the systems they administer when requested by authorized UTMB management
  - must cooperate with authorized UTMB management investigating security incidents
# Account Management, continued

## Practice Standards (con’t)

- **Owners:**
  - are responsible for developing transition plans for departmental data
  - are responsible for timely notification to appropriate parties when staff leaves department
  - are responsible for periodically reviewing access provided to users based on job and functional requirements (access review may be delegated to a Trusted Requestor)

- **Trusted Requestors:**
  - are responsible for requesting revocation of all accounts for personnel transferring from their department or terminating employment at UTMB at the time of separation
  - are responsible for assessing the separating employee’s non-shared drives and removing departmental information prior to employee separation
  - are responsible for requesting minimum necessary access for employees within their department that enables them to perform their job functions

- **Vendor and special access accounts must be reassessed semi-annually.**

- **Students will retain their email address and MyStar access for 180 days following graduation.**

## 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
- UTMB IR Security Management Practice Standards Approval Process
- UTMB IR Password Management Practice Standard