Section 1	Security Management	09/03/02	-Effective
Subject 2	Access Management	07/08/09	-Revised
Practice Standard 1.2.3	**Special Access**	Information Security Officer-Author	

Special Access

Introduction

Technical support staff, security administrators, system administrators, and others may have special access account privilege requirements as compared to typical or normative users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling, and monitoring these accounts is extremely important to an overall security program.

Purpose

The purpose of the UTMB Special Access Practice Standard is to establish the rules for the creation, use, monitoring, control, and removal of accounts with special access privilege.

Audience

The UTMB Special Access Practice Standard applies equally to all individuals who have, or may require, special access privilege to any UTMB Information Resources (IR).

Implications

- All multi-user computer and network systems must support a special type of User ID which has broadly-defined system privileges. This Used ID enables access to authorized individuals and processes of system; therefore, these privileges must be restricted and granted only to those directly responsible for system management and/or security.
- The extent of access privileges granted or used should not exceed that which is necessary to accomplish a specific business objective.

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).

Section 1	Security Management	09/03/02	-Effective
Subject 2	Access Management	07/08/09	-Revised
Practice Standard 1.2.3	**Special Access**	Information Security Officer-Author	

Special Access, *continued*

Practice Standards

- Systems must be administratively supported and maintained by personnel that are properly trained and technically competent.
- All users must sign the UTMB Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
- Each individual who uses special access accounts must refrain from abuse of privilege and must only conduct investigations under the direction of the ISO.
- Each individual who uses special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
- Each account used for special access must meet the UTMB Password Management Practice Standard.
- UTMB departments must submit to CIRT a list of administrative contacts for their systems that are connected to the UTMB network and must provide updates as contact changes occur.
- The password for a shared special access account must change when an individual with the password leaves the department or UTMB, or upon a change in the vendor personnel assigned to the UTMB contract. The account must also be re-evaluated as to whether it should remain a shared account or not. (Shared accounts must be kept to an absolute minimum.)
- In the case where a system has only one administrator, a password escrow procedure must be in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
- When special access accounts are needed for audit, software development, software installation or other defined need, they:
  - must be authorized by the system owner, IRM, or ISO
  - must be created with a specific expiration date
  - must be removed when work is complete
- All privileged commands issued in association with special access must be traceable to specific individuals via the use of comprehensive logs.

Section 1	Security Management	09/03/02	-Effective
Subject 2	Access Management	07/08/09	-Revised
Practice Standard 1.2.3	**Special Access**	Information Security Officer-Author	

Special Access, *continued*

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 *Information Resources Security Policy*
- UTMB IR *Security Glossary*
- UTMB IR *Security Management Practice Standards Approval Process*
- UTMB IR *Password Management Practice Standard*
- UTMB IR *Security Monitoring Password Standards*
- UTMB IR *Security Procedures – Password Escrow*