Physical Access

Introduction Technical support staff, security administrators, system administrators and others may have Information Resource (IR) physical access requirements as part of their function. The granting, controlling and monitoring of the physical access to IR and IR facilities is extremely important to an overall security program.

Purpose The purpose of the UTMB Physical Access Practice Standard is to establish rules for the physical securing of IR facilities and hardware.

Audience The UTMB Physical Access Practice Standard applies to all individuals within the UTMB enterprise who are responsible for the installation and support of IR, individuals charged with IR Security and data owners.

Implications
- All mission critical computer and communications systems shall be physically located within the protected confines of a secured information resources facility.
- Access to mission critical IR facilities shall be physically restricted, managed, and documented.
- Workstations should be used in a manner that maximizes the security of the information contained therein, especially in high traffic areas.
- Reviews of physical security measures for information resources shall be routinely conducted.

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).
Physical Access, continued

- Access to IR facilities must be granted only to UTMB support personnel whose job responsibilities require access to that facility.
- The process for granting access to IR facilities must include the approval of the manager responsible for the facility.
- Requests for access must come from the applicable UTMB data/system owner.
- Support personnel must not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when authorized persons go through these entrances. (Where access is card controlled, each individual must use their own card to gain entry.)
- All IR facilities that allow access to visitors will track visitor access with a sign in/out log.
- Visitors must be escorted in access controlled areas of IR facilities.
- Card access records and visitor logs for mission critical IR facilities must be kept a period of one year for review and audit purposes and must minimally contain sign-in date, time in, time out, UTMB badge number or company name, reason for visit (maintenance performed if applicable), printed name, signature, and accountable party who authorized entry.
- The manager responsible for the IR facility must review physical access rights, access records and visitor logs for the facility on a periodic basis and remove access for individuals who no longer require access.
- When an individual changes roles or separates from UTMB, all physical security access codes known by the individual must be deactivated or changed (i.e., the password entered on a cipher lock to get into the IR facility must be changed) and all access rights must be immediately disabled.
- All individuals granted physical access to IR facilities shall abide by the recommended requirements outlined within this practice standard and shall not bypass or circumvent prescribed security measures.
- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.
- All multi-user computer and communications equipment must be located in locked rooms to prevent tampering and unauthorized use.
Physical Access, continued

Practice Standards (con’t)

- Workstations, monitors and other IR should be setup and/or located in a way as to protect the IR from loss or theft, for example, setup workstations under desks or in credenzas and use cable guides or locks to secure monitors and printers.

- If there has been no activity on a computer terminal, workstation, or microcomputer (PC) for ten (10) minutes, the system must automatically terminate the session or invoke a password enabled screensaver. Authentication to re-establish the session must occur after lockout due to idle time.

- If the computer system to which they are connected, or which they are currently using, contains sensitive information or can be used to access other information resources on the UTMB network, users must not leave their microcomputer (PC), workstation, or terminal unattended without first logging-out or invoking a password enabled screensaver, unless physical access is otherwise assured (e.g., a locked private office).

- All computer/magnetic storage media (i.e., hard disk, floppy disk, optical disk, magnetic tape/cartridge, etc.) containing sensitive information must be physically secured when not in use.

- Special care should be taken with portable IR (laptops, flash drives, portable hard drives, etc.) to protect against loss or theft, for example, use cable locks to secure laptops, use encrypted flash drives, etc.

- Prior to disposal or transfer of ownership, all stored data must be destroyed or permanently removed from any computer/magnetic storage media (i.e., hard disk, floppy disk, optical disk, magnetic tape/cartridge, etc.).

- Information resources assigned to UTMB from another agency shall be protected in accordance with the conditions imposed by the providing agency. Conversely, information resources assigned from UTMB to another agency shall be protected in accordance with the conditions imposed by UTMB.

- All physical security measures must comply with applicable statutes, standards, and regulations.
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