Vendor Access

Introduction
Vendors play an important role in the support of hardware, software, management and operations for customers. Vendors can remotely view, copy and modify data; correct software and operating systems problems; monitor and fine tune system performance; monitor hardware performance and errors; modify environmental systems; and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to UTMB.

Purpose
The purpose of the UTMB Vendor Access Practice Standard is to establish the rules for vendor access to UTMB Information Resources (IR) and support services (air conditioning, uninterruptible power supply, power-distribution units, fire suppression, etc.), vendor responsibilities, and protection of UTMB information.

Audience
The UTMB Vendor Access Practice Standard applies to all individuals who are responsible for the installation of new IR assets, the operations and maintenance of existing IR, and who facilitate vendor access for maintenance, monitoring, and troubleshooting purposes.

Implications
- All third party access to UTMB internal computer systems which are not clearly public must be approved in advance by the IRM or their designee. (They should be treated very carefully on a case-by-case basis.)
- In-bound dial-up or Internet privileges must not be given to third party vendors unless the relevant system manager determines that these vendors have legitimate business need for such access. These privileges must be enabled for specific individuals and only for the time period required to accomplish approved tasks.
- As a condition of gaining access to UTMB’s computer network, every third party must secure its own connected systems in a manner consistent with UTMB’s requirements.
Vendor Access, 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

- Vendors must comply with all applicable UTMB policies, practice standards, and agreements, including, but not limited to:
  - Safety Policies
  - Privacy Policies
  - Security Policies
  - Auditing Policies
  - Software Licensing Policies
  - Acceptable Use Policies
  - Email Use and Internet Use Policies
  - IR Security Management Practice Standards
- Vendor agreements and contracts must specify:
  - the UTMB information the vendor should have access to
  - how UTMB information is to be protected by the vendor
  - acceptable methods for the return, destruction or disposal of UTMB information in the vendor’s possession at the end of the contract
  - the vendor must only use UTMB information and IR for the purpose of the business agreement
  - any other UTMB information acquired by the vendor in the course of the contract cannot be used for the vendor’s own purposes or divulged to others
- Each vendor must provide UTMB with a list of all employees working on the contract. The list must be updated and provided to UTMB within 24 hours of staff changes pertinent to physical or logical access concerns.
Vendor Access, continued

- Any person or organization (vendor) that conducts business on behalf of UTMB that may create, receive, maintain, or transmit Individually Identifiable Health Information (IIHI) or Protected Health Information (PHI) as defined by HIPAA must have a properly executed Business Associates Agreement (BAA) on file with the Office of Institutional Compliance.

- Each on-site vendor employee must acquire a UTMB identification badge that will be displayed at all times while on UTMB premises. The badge must be returned to UTMB when the employee leaves the contract or at the end of the contract.

- Each vendor employee with access to UTMB confidential and/or sensitive information must be approved to access that information compliant with applicable IR Security Management Practice Standards.

- Vendor personnel must report all security incidents directly to the Computer Incident Response Team (CIRT) at (409) 772-3838 or cirt@utmb.edu.

- If vendor management is involved in UTMB incident management, the details must be specified in the contract.

- Vendor must follow all applicable UTMB change management processes and procedures.

- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate UTMB management.

- All vendor maintenance equipment on the UTMB network that connects to the outside world via the network, telephone line or leased line and all UTMB IR vendor accounts will remain disabled except when in use for authorized maintenance.

- Vendor access must be uniquely identifiable, and password management must comply with the UTMB Password Management Practice Standard and Special Access Practice Standard. Vendor’s major work activities must be entered into a log and available to UTMB management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, and deliverables.

- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and/or destroyed within 24 hours.

- Upon termination of contract or at the request of UTMB, the vendor will destroy all UTMB information and provide written certification of that destruction within 24 hours.
Vendor Access, continued

Practice Standards (con’t)
- Upon termination of contract or at the request of UTMB, the vendor must surrender all UTMB identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized UTMB management.
- Vendors are required to comply with all Federal, State and other regulatory auditing requirements, including the auditing of the vendor’s work.
- All software used by the vendor in providing service to UTMB must be properly inventoried and licensed.

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 Email Use Policy
- UTMB Internet Use Policy
- UTMB IR Security Glossary
- UTMB IR Security Management Practice Standards Approval Process
- UTMB IR Security Monitoring Practice Standard
- UTMB IR Password Management Practice Standard
- UTMB IR Account Management Practice Standard
- UTMB IR Special Access Practice Standard