Portable Computing

Introduction
A portable computing device is any easily transportable device that is capable of storing and/or processing data. They include, but are not limited to: laptops, smart phones, USB drives, CD/CDR/DVD/Blu-ray disks, etc. Their small size, functionality and ease of use make them very desirable to personnel who need to be mobile while addressing the business of UTMB. However, the portability offered by these devices increases the security exposure due to their propensity for loss or theft.

Purpose
The purpose of the UTMB Portable Computing Practice Standard is to establish rules for the use of portable devices and means to protect the data they may hold. These rules are necessary to preserve the integrity, availability, and confidentiality of UTMB information.

Audience
The UTMB Portable Computing Practice Standards apply equally to all individuals that utilize portable computing devices and access UTMB Information Resources.

Implications
Regarding information security, the user is expected to have a heightened awareness and take appropriate precautions while using portable devices to access UTMB IR.

Privacy
Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of UTMB are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 1 TAC §202 (Information Security Standards), UTMB Information Resource Standards and in the University of Texas System, UTS 165 - Information Resources Use and Security Policy.

Sensitive Digital Data Management
Confidential digital data, as defined by UTS 165, includes social security numbers, Protected Health Information (PHI), confidential research data, digital data associated with an individual and/or digital data protected by law. Confidential digital data must be secured and protected while at rest (electronic storage on any type of storage device), mobile (laptop, smart phones or USB drives) and in transit (via email or the Internet).
Portable Computing (Continued)

**Practice Standards**

- Only UTMB approved portable computing devices may be used to access UTMB Information Resources.
- Portable computing devices must be configured in accordance with Practice Standard 1.1.5, Platform Hardening and secured with full disk encryption.
- Non-UTMB laptops that are used to conduct UTMB business must have full disk encryption and password protection enabled.
- Confidential data should not be stored on portable computing devices. In the event that there is no alternative to local storage, explicit approval by the Information Security Officer and the data owner must be obtained prior to storing the data on the device.
- When flying aboard commercial airlines, users must not check portable computing devices as baggage. The devices must remain in the possession of the traveler as hand luggage.
- Confidential data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.
- Critical UTMB data stored on portable computing devices must not be used as the single source for that data, i.e., UTMB data stored on portable devices must be a copy or backed up in accordance with Practice Standard 1.3.2, Backup/Data Recovery.
- All lost, stolen or compromised devices must be reported to the Information Security Officer in accordance with Practice Standard 1.4.1, Reporting of Lost or Stolen Information Resources and Data
- Unattended portable computing devices must be physically secure. This means they must be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.
- UTMB owned laptops that are past their service life should be returned to the IS Depot for processing and disposal.

**Disciplinary Actions**

Violation 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.
Portable Computing (Continued)

References

- Texas Administrative Code, Chapter 202
- University of Texas System, UTS-165 Information Resource Use and Security Policy
- Security Practice Bulletin #1, Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices
- DIR Practices for Protecting Information Resources Assets
- DIR Standards Review and Recommendations Publications