TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER
EL PASO

TTUHSC El Paso User Agreement for Removable Media

As an asset custodian, I recognize the risk involved with using a mobile storage device and I acknowledge that I have read, become familiar with, and will adhere to IT security protocols of protected information. As an asset custodian, I recognize and acknowledge that circumventing security protocols can result in sanctions imposed by TTUHSC El Paso, state, and federal entities. I also recognize that by signing this document, I accept risk associated with the use of the type of digital media I am requesting privilege to use. Failure to comply with acknowledgements as mentioned in this document as well as failure to disclose the type of media use requested increases the risk I absorb as well as sanctions imposed.

According to IT Security policies and protocols, TTUHSC El Paso shall implement effective controls to:

- Ensure that adequate privacy protection requirements are in place to minimize overall privacy risk,
- Employ malicious code protection mechanisms at system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code,
- Manage risk to organizational operations and assets, individuals, other organizations associated with the operation and use of systems,
- Ensure asset custodians protect physical digital media using encryption mechanisms as outlined in IT security processes,
- Ensure asset custodians adhere to access restrictions to digital and non-digital media.

Expected protocols for acceptable use of digital media includes but is not limited to:

(a) Loss / Theft. Immediately notify TTUHSC El Paso management if a mobile device is lost or stolen and the user must alert management to the circumstance of the loss and the data contained on the mobile device;
(b) Conduct. Users must conduct themselves in accordance with TTUHSC El Paso's Acceptable Use parameters;
(c) Encryption. The mobile device must be encrypted according to IT Security Standards.
(d) Wireless: Users are required to utilize good judgment when connecting the mobile device to other devices and networks:
    i. Bluetooth: Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices.
    ii. WiFi: Users may use only secure (e.g., WPA2) WiFi networks known to be trustworthy.
    iii. Cellular: TTUHSC El Paso is not responsible for overages or data plans for cellular usage.
(e) Data Handling. Asset custodians are required to follow guidelines for data handling as described below.

DATA HANDLING GUIDELINES

The following data handling guidelines were shortened for this acknowledgement; the original data classification and data handling guidelines are located at http://elpaso.ttuhsc.edu/it/policies/default.aspx.

Handling Controls	Restricted/Regulated	Confidential	Internal Use	Public
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible	*No special requirements*
Storage Media (Hard Disk Drives (HDDs), Flash drives, tapes, CDs/DVDs, etc.)	▪ Physically destroy the hard drives and media ▪ Requires use of company-approved vendor for destruction	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of the media is not sufficient)	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media

I recognize that I am bound by the IT security policy requirements as well as TTUHSC El Paso policies that govern the use, access, storage, and management of protected data. I acknowledge that I will abide by the necessary data handling guidelines.

Type of media requested: _____

_____ _____

Signature of Applicant Date

_____ _____

Signature of Department Head Date

_____ _____

IT Security Witness Date