TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER AT EL PASO

Operating Policy and Procedure

HSCEP OP: 56.01, 1.4.14 PORTABLE COMPUTING

PURPOSE:

REVIEW:

POLICY/PROCEDURE:

Security Guidelines

Portable Computing Devices are inherently at risk for theft and security vulnerability. In cases where there is a justifiable business need or requirement for confidential information, such as patient information, confidential student information, grades, etc., to be stored or transferred to a Portable Computing Device appropriate security measures shall be implemented as listed below.

Security Policy

- Confidential information shall not be stored, downloaded, or leave the Institution unless there is a need to access this information away from the Institution. Authorization will need to be obtained by each individual from the information owner. Information owner responsibilities, definition, and more information can be found in Policy 1.1, I.T. Resource Management and Responsibilities.
- Confidential information shall not be shared with others who do not have a job-related need for this information.
- Confidential information should not be copied to or stored on a portable computing device, removable media, or a non-state owned computing device that is not encrypted.
- The Portable Computing Device shall be password protected using the security feature provided on the Portable Computing Device and there should be no sharing of the password.
- Portable Devices owned by TTUHSC El Paso shall be hardened according to CIS Level 1 baselines and the information custodian is responsible for attaining related benchmarks from TTUHSC El Paso IT Information Security.
- Removable media such as memory cards must not be used to store confidential information.
- A Desktop PC that is used for synching must have approved antivirus software installed, and require user log on.
- Whenever there is no longer a job related need to access or store this confidential information, it must be deleted