TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.10.07 - Server Hardening

PURPOSE: To define the process for deploying and maintaining servers in a secure state.

REVIEW: This policy will be reviewed once a year by the director of Systems and Network Operations and the information security officer (ISO) and will be approved by the chief information officer (CIO).

POLICY / PROCEDURE

A server cannot be connected to the TTUHSC at El Paso network until it is in an approved, secure state. Prior to connecting the server to the network, the following must be performed:

- Install the operating system from an IT-approved source, which includes proper licenses
- Reserve IP address and update IP manager software
- Remove all unnecessary software, system services, and drivers
- Set appropriate security parameters, file protections, and enable audit logging
- Disable or change the passwords for default accounts
- Register all new servers on a server creation log
- Install IT-approved anti-virus software
- Apply the latest vendor supplied patches after testing for compatibility with the production environment
- Ensure servers are hardened to CIS level I baselines

Formatted: Font: (Default) Arial, 10 pt, Font color: Auto

All servers are required to be submitted to a vulnerability assessment performed by the TTUHSC El Paso Information Technology Security group (ITSec) prior to use.

Formatted: Font: (Default) Arial, 10 pt, Font color: Auto

In the event that a vulnerability or a combination of vulnerabilities constituting an unacceptable level of risk (as deemed by ITSec) is identified, the systems group will be responsible for ensuring the vulnerabilities are addressed. Any such risk must be addressed prior to production use. Further scanning may be required.

ITSec will monitor security issues, both internal and external, and the release of security patches on behalf of TTUHSC El Paso. After the systems group is notified by ITSec, patches must be implemented within a specified timeframe determined by the security level of the patch, or the risk level of the vulnerability. ITSec will routinely monitor to ensure the system(s) is/are in compliance. Failure to comply with these guidelines can result in the server(s) being removed from the network.