TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.50.16 **– Patch Management**

CONTROL OBJECTIVE: TTUHSC El Paso system developers and integrators are required to create and implement Threat Analysis and Flaw Remediation plans and initiatives as advocated by the State and Federal Regulations.1 This policy is to serve as a means of protecting and maintaining TTUHSC El Paso systems, infrastructure, network and Information Resources from vulnerabilities, breaches, and other threats in a timely and secure manner.

REVIEW: This policy will be reviewed and updated in March of every Odd Numbered Year (ONY) by the Information Security Officer (ISO) and the Chief Information Officer (CIO), or when necessary as dictated by governing entities.

POLICY/PROCEDURE:

The following are areas of focus but are not exhaustive procedures and guidelines for Patch Management.

Threat Analysis [2]

- Asset custodians and data/process owners are required to:
  a) Address new threats and vulnerabilities on an ongoing basis and ensures these applications are protected against known attacks by either of the following methods:
     i. Reviewing applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or
     ii. Installing an application firewall.
  b) Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows:
     i. At least annually;
     ii. After any changes;
     iii. By an organization that specializes in application security;
     iv. That all vulnerabilities are corrected; and
     v. That the application is re-evaluated after the corrections

Vulnerability Scanning [3]

- The organization :
  a) Scans for vulnerabilities in systems and hosted applications and when new vulnerabilities potentially affecting the system/applications are identified and reported;
  b) Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards by:
     i. Enumerating platforms, software flaws, and improper configurations;
     ii. Formatting and making transparent, checklists and test procedures; and
     iii. Measuring vulnerability impact;
  c) Analyzes vulnerability scan reports and results from security control assessments;
  d) Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk; and
  e) Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other systems (e.g., systemic weaknesses or deficiencies).
  f) TTUHSC El Paso's vulnerability management team is solely responsible for approving

and overseeing the use of any enterprise scanning and assessment tools. The use of any other vulnerability scanner is prohibited without prior, written approval by the vulnerability management team.

Flaw Remediation [4]

- The organization :
  a) Employs weekly patch maintenance schedule update patches or fixes as available on institutional computing devices per findings of tools and vulnerability scans.
  b) Regular maintenance shall include but is not limited to: institutional systems, servers, file shares, et cetera.
  c) In the event an extended amount of time is needed for patching, IT provide notification regarding downtime via email notification.
  d) System owners and system custodians are responsible for implementing appropriate mitigations and recommendations according to baseline configurations outlined in CIS level 1 benchmarks.

SANCTIONS:

Interference with patch management and flaw remediation efforts by any employee, student, or vendor, may result in the disciplinary actions as defined in HSCEP Information Technology Policy 56.01.10. 5

All other IT Policies can be found at https://ttuhscep.edu/it/policies/

1. TAC 202.74
2. NIST 800-53 SA-11(a) Threat Analysis & Flaw Remediation
3. NIST 800-53 RA-05 Vulnerability Scanning
4. TTUHSC El Paso Antivirus Procedure & Maintenance Schedule
5. 56.01.10 Disciplinary Process