Overview

This document describes the UTHSC Patch Management Process. This document is designed to offer procedures for the protection of all mission critical and PHI applications and data.

Vulnerabilities can occur when a particular combination of technologies do not work properly when used together. Vulnerabilities can also be the result of an oversight in software production by the manufacturer. Every vulnerability is potentially a target for intrusion or other malicious activity. The key is to patch, and to patch early, before intruders use details of the exploit to gain access to a system.

Purpose

This process is enacted to:

- keep all necessary patches on servers, network devices, workstations, laptops and other mobile devices
- document and log all changes
- manage timely changes through the change control process prioritized by the severity of vulnerability.

Scope

This addendum applies to all devices that use, store, process, report, etc., applications and data. Included in this policy are devices that store:

- UTHSC mission critical applications and data
- UTHSC Protected Health Information applications and data

Policy

- **Implement latest patches and updates** - All devices, workstations, servers, printers, etc., must be kept at the latest non-damaging patch levels for the operating system installed.
- **Subscribe to advisory and alert lists -** These will alert you to any new software updates or patches that are released. Check out the following resources for more information:
    - **Manufacturers' Web sites –** Many software providers will offer a notification list to their customers and these providers will have the information posted on their Web site.

- **Independent bug-tracking sources –** Sign up for the CERT Coordination Center's Advisory List, the BugTraq mailing list, or visit Security Focus or other bug-tracking sources regularly.

- **Document everything.** As patches are considered, implemented and tested, every step should be documented so that there is a complete audit trail in case anything is called into question in the future. Documentation should be maintained in bound notebooks or equivalent means and should be stored in a physically protected and secure manner in a secure area.

- **Determine the relevance and severity of vulnerability.** One should review advisories and alerts within 24 hours of receipt and should determine if any are applicable to the operation. If so, decide the severity of the issue immediately.

- **Separate reviewer from patch applicator.** The person that is reviewing the advisories and making determinations should not be responsible for applying the patch. If the same person shares those duties, one runs the risk of biased opinions. The person who has to apply the patch may tend to gloss over the advisories, knowing if there is a severe risk found, it will need to be fixed on his or her time. If your reviewer is removed from the situation, one will be more likely to obtain a fair judgment.

- **Test patch before deploying it.** Sometimes the patches themselves can cause additional or unforeseen operational and security issues in an enterprise. Apply the patch first in a test environment to make sure that the patch itself will not introduce a new vulnerability or disrupt normal business functions in any way.

Enforcement

Reference Enforcement **in Acceptable Use document**

Additional Information

Any inquiries relating to this Patch Management Policy should be directed to the Security Director.