THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: RM-003-Patch Management	
Version 3	**Effective Date: 10/07/2020**

Responsible Office: Office of Cybersecurity	Last Review: 03/16/2022 Next Review: 03/16/2024
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To provide an ongoing and consistent system and application update program that supports regular security updates and patches to operating systems, firmware, productivity applications, and utilities. Updates are critical to maintaining a secure operational environment.

Scope

This Standard applies to all UTHSC IT Resources including, but not limited to, operating systems, applications, endpoints, and servers connected to the UTHSC network.

Definitions

Endpoint – A device that exists at the end of a network connection, i.e., a desktop, laptop, mobile phone or Internet of Things (IoT) device.

IT Resource - Any data, device, or other component of the information environment that supports information-related activities. Assets generally include hardware (e.g., servers and switches), software (e.g., mission critical applications and support systems) and information.

ITS – the Information Technology Services department of UTHSC

System owner - Person or organization that has responsibility for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of an information system

Patch – A piece of software designed to fix problems with, or update a computer program, or its supporting data. Patches include, but not limited to, updating software, fixing a software bug, installing new drivers, addressing new security vulnerabilities, and addressing software stability issues.

Responsibilities

Office of Cybersecurity is responsible for conducting scans of IT Resources to identify vulnerabilities.
ITS Infrastructure Division is responsible for deploying endpoint patches and updates to operating systems, networking components and certain applications.
System Owner, the person ultimately response for the system, is responsible for managing and remediation of the identified vulnerability, with the assistance of ITS or the data custodian.
System Custodian is responsible for applying required and suggested security controls based on the classification, designated in GP-005-Data Security.
End User (UTHSC Campus Community) who has the custody and responsibility of a UTHSC endpoint and is responsible for having the device available to receive updates.

Standard

1. Automatic security patching is required where applicable.
2. System owners and administrators must monitor all applicable vendor informational sites on a regular basis to stay aware of when operating system and application patches are made available.
3. Risk assessments must be performed, for patches or changes deemed to be significant, to address potential negative impact to confidentiality, integrity, or availability of the UTHSC IT Resource in accordance with RA-001-Risk Assessment and change management processes.
4. New devices must be patched to a supported version. No device should be on the UTHSC network whose operating system or applications are past end of life (EoL).
5. Patches should be tested in an appropriate dev/test environment, when available, to understand the impact of deploying the patch in the production environment. This is required for patches that, in the event of a failure or unexpected issue, could result in a significant impact to the University.
6. Prior to production deployment, a back out plan must be in place to roll back changes in the event the patch causes issues with the production environment.
7. System components and devices attached to the UTHSC network must be regularly maintained by applying security patches in a timely manner. The

scheduling these patches is based on the severity level of the vulnerability as follows:

Severity Level	Deadline
Critical	15 days
High	15 days
Medium	90 days
Low	180 days

8. A system reboot is required to successfully install most security patches. These reboots should be automated whenever possible. Patches are not considered applied until the reboot happens, if applicable.
9. If a different schedule is needed for updating a specific device or group of devices, ITS will work with the system owner to set up a schedule that is beneficial. There must be some set schedule for the device to remain on the UTHSC network.
    a. Other exceptions to this schedule will occur as needed. i.e. emergency patching
10. Exceptions to this Practice should be requested using the process outlined in GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices. Exceptions must enumerate mitigating controls that will be put in place to reduce the risk to the system and data until the patch can be applied.

References

1. RA-001-Risk Assessment
2. GP-005-Data Security
3. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices
4. NIST Glossary of Terms