THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: RM-002-Vulnerability Management	
Version 4	**Effective Date: 04/18/2018**

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 establish rules and principles for identifying and managing vulnerabilities in IT Resources. IT Resources contain inherent weaknesses that are termed as vulnerabilities. Threats exploit vulnerabilities to cause harm to IT Resources. Hence, it is imperative to regularly identify, and remediate vulnerabilities and prevent occurrences of security incidents.

Scope

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

Definitions

IT Resource - Any data, device, or other component of the digital 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.

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

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

UT Health Science Center: RM-002-Vulnerability Management	
Version 4	**Effective Date: 04/18/2018**

Responsibilities

Office of Cybersecurity is responsible for conducting scans of IT Resources to identify vulnerabilities.

System owner is responsible for the managing and remediation of the identified vulnerability, with the assistance of the Patch Management Team.

Patch Management Team in ITS' Infrastructure Division is responsible for applying certain security patches and updates.

Standard

1. Information Technology Services (ITS) and the Office of Cybersecurity has a goal to provide secure IT systems and services in order to protect organizational information assets, as well as the privacy of employees, students, contractors, and other members of the UTHSC community.
2. The timely and consistent application of vendor-supplied security patches or mitigation of a reported vulnerability are critical components in protecting the network, systems, and data from damage or loss due to threats such as worms, viruses, data loss, or other types of external or internal attacks.
3. The Office of Cybersecurity shall conduct routine scans of its website, servers, and devices connected to its networks to identify operating system and application vulnerabilities on those devices.
4. System Owners or administrators are required to routinely review the results of vulnerability scans and evaluate, test, and mitigate operating system and application vulnerabilities appropriately. Upon discovery, vulnerabilities should be mitigated in a timely manner, 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

5. Should an owner or administrator identify a reported vulnerability as a potential false positive, the Office of Cybersecurity should be notified immediately.

6. Any risk not accepted regarding systems with known vulnerabilities that cannot be patched must have documented compensatory controls in place to remediate the vulnerabilities. Minimally every 6 months these systems must be reevaluated.
7. UTHSC IT Resources that are unable to be secured because they are outdated or unsupported must be replaced or removed from the UTHSC network unless an approved exception has been obtained.
8. Exceptions to this Practice should be requested using the process outlined in GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices

References

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