THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: IT7810-HSC-A Vulnerability Management	
Version 6	**Effective Date: 04/18/2018**

Responsible Office: Office of Cybersecurity	Last Review: 03/01/2025 Next Review: 03/01/2027
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, known as vulnerabilities. Vulnerabilities can lead to threats that could be exploited to cause harm to the confidentiality, integrity, and availability of IT Systems and Resources. Hence, it is imperative to regularly identify and remediate vulnerabilities to prevent occurrences of security incidents.

This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

This Standard applies to all University of Tennessee Health Science Center (UTHSC) IT Resources, including, but not limited to, operating systems, applications, endpoints, and services connected to the UTHSC network.

Definitions

UTHSC Information Technology (IT) Resource - a broad term for all things related to information technology from a holistic point of view and covers all University-owned or managed information technology services, including cloud-based services, that users have access to.

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.

Responsibilities

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

System Custodian is responsible for the maintenance and operations of the technological infrastructure, including network or applications, to support running the system(s) supporting University activities. The system custodian should know the system assets and technical operations and be able to advise on the technical impact of a compromised system.

System Owner is a senior stakeholder within the University system who is responsible for ensuring that technology system functions meet University goals and adhere to University policies and standards. Working with the System Custodian, ITS Risk Management Function, and Cybersecurity Function, they should identify the potential threats to a system, conceptualize risk scenarios, and determine risk likelihood and impact.

System owners and custodians are responsible for managing and remediating 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. Applying vendor-supplied security patches and mitigating reported vulnerabilities in a timely and consistent manner is essential to protecting networks, systems, and data from threats such as malware, unauthorized access, and cyberattacks.
2. The Office of Cybersecurity conducts routine vulnerability scans of UTHSC websites, servers, and network-connected devices to identify security risks.
3. A Penetration Testing program is developed and maintained in order to identify vulnerabilities that might not be detected by automated vulnerability scanning.
4. System Owners and Custodians must review scan results and take appropriate actions to evaluate, test, and remediate vulnerabilities within the following timelines based on severity:

Severity Level	Deadline
Critical	14 days
High	14 days

Medium	90 days
Low	180 days

5. If a system owner or custodian identify a reported vulnerability as a potential false positive, they must notify the Office of Cybersecurity immediately.
6. Risks must either be accepted or addressed through documented mitigation plans in accordance with IT0004-HSC-A.01-Risk Assessment Process.
7. UTHSC IT Resources that cannot be secured because they are outdated or unsupported must be replaced or removed from the UTHSC network unless an approved exception has been obtained or additional mitigating controls have been put in place.
8. Exceptions to this Practice should be requested using the process outlined in IT0003-HSC-A.02-Security Exceptions and Exemptions to ITS Standards Practice & Controls.

Policy History

Version #	Effective Date
1	04/108/2018
2	05/27/2021
3	10/07/2021
4	05/17/2022
5	01/11/2023
6	03/01/2025 – new naming convention

References

1. IT0003-HSC-A.02-Security Exceptions and Exemptions to ITS Standards Practices & Controls
2. IT0004-HSC-A.01-Risk Assessment Process
3. NIST Glossary of Terms