THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

| UT Health Science Center:<br>RM-002-Vulnerability Management | |
|---|---|
| Version 5 | Effective Date: 04/18/2018 |

| | |
|---|---|
| Responsible Office: Office of Cybersecurity | Last Review: 07/27/2023<br>Next Review: 07/27/2025 |
| Contact: Chris Madeksho | Phone: 901.448.1579<br>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 in order 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 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 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.
**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 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, and other types of external or internal attacks.
3. The Office of Cybersecurity conducts routine scans of UTHSC websites, servers, and devices connected to its networks to identify operating system and application vulnerabilities on those devices.
4. A Penetration Testing program is developed and maintained in order to identify vulnerabilities that might not be detected by automated vulnerability scanning.

5. System Owners or Custodians 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 |

6. Should a system owner or custodian identify a reported vulnerability as a potential false positive, the Office of Cybersecurity should be notified immediately.
7. Risks must either be accepted or have mitigation plans documented in accordance with RM-001.01-Risk Assessment Process.
8. 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 or additional mitigating controls have been put in place.
9. 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. RM-001.01-Risk Assessment Process
2. GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices
3. NIST Glossary of Terms