THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: IT7810-HSC-E Antivirus_Antimalware Protection	
Version 3	**Effective Date: 03/17/2016**

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 ensure that proactive security measures are taken to prevent and detect malicious software and that awareness is raised for recognizing and immediately reporting suspected occurrences of malicious software.

Scope

This Practice applies equally to all University of Tennessee Health Science Center (UTHSC) IT Resources and to all members of the UTHSC community, contractors, and others who process, store, transmit, or have access to these UTHSC IT Resources.

Definitions

Endpoint – A device at the end of a network connection, i.e. a desktop, laptop, or mobile phone.
EDR – Endpoint Detection and Response software
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.
Malware – Any software intentionally designed to cause damage. Types of malware include viruses, worms, Trojan horses, ransomware, spyware, adware, and rouge software.
Virus – A type of computer program that can replicate and spread after an initial execution.

Responsibilities

Customer Technology Services (CTS) is responsible for ensuring that endpoints are enrolled in the approved endpoint management software per IT0102-HSC-B-Device Life Cycle Security.
Office of Cybersecurity is responsible for the deployment of UTHSC's approved EDR to those endpoints enrolled in the approved management software.

End User (UTHSC Campus Community) is responsible for recognizing and immediately reporting suspected occurrences of malicious software.

Practice

1. All UTHSC IT Resources must have installed the approved EDR software.
2. Malicious software protection controls:
   a. Must not be disabled or bypassed without formal documented exception per IT0003-HSC-A.02-Security Exceptions and Exemptions to ITS Standards Practices & Controls.
   b. Must not be altered in a manner that will reduce the effectiveness of the controls.
   c. Must not be altered to reduce the frequency of automatic updates.
3. The Office of Cybersecurity shall ensure that:
   a. EDR software protection controls are installed on every UTHSC endpoint.
   b. Updates from the EDR are received in the console and automatically pushed out to the endpoints as part of a scheduled maintenance cycle.
   c. All software is scanned for malicious components using up-to-date protection controls before being loaded on any computing device.
   d. If the EDR software detects malware, it remediates the incident and notifies the Office of Cybersecurity based on established security controls and policies.
   e. Ensure that all cloud-based services have a malware defense program.
4. The end user shall have the responsibility to:
   a. Never disable anti-malware software on UTHSC IT Resources.
   b. Use reasonable precautions to prevent malicious software to a computing device when importing data through physical (USB devices, memory cards) or electronic means (email, downloading from the Internet).
   c. Ensure that all portable computing devices or personal computers in their custody are running industry-recognized malicious software protection controls.
   d. Immediately report any suspected or actual incidence of malicious software infection as a security incident per IT0017-HSC-A-Security Incident Response.

UT Health Science Center: IT7810-HSC-E Antivirus_Antimalware Protection	
Version 3	**Effective Date: 03/17/2016**

Policy History

Version #	Effective Date
1	03/17/2016
2	01/25/2023
3	03/01/2025 – new naming convention

References

1. IT7810-Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy
2. IT0003-HSC-A.02-Security Exceptions and Exemptions to ITS Standards Practices & Controls
3. IT0017-HSC-A-Security Incident Response
4. IT0102-HSC-B-Device Life Cycle Security