THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

| UT Health Science Center:<br>GP-007.02-Antivirus_Antimalware Protection | |
|---|---|
| **Version 1** | **Effective Date: 03/17/2016** |

| | |
|---|---|
| Responsible Office: Office of Cybersecurity | Last Review: 11/10/2020<br>Next Review: 11/10/2022 |
| Contact: Chris Madeksho | Phone: 901.448.1579<br>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 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 that exists at the end of a network connection, i.e. a desktop, laptop, or mobile phone.
**EDR** – Endpoint Detection and Response software
**IT Resource** - Any data, device, or other component of the information environment that supports information-related activities. Assets generally include hardware (e.g. endpoint devices), software (e.g. mission critical applications and support systems) and information.
**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 that endpoints are enrolled in the approved endpoint management software per CS-001 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 GP-001.02-Security Exceptions and Exemptions to ITS Standards and Practices.
   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 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 notify the Office of Cybersecurity based on established security controls and policies.
4. The end user shall have the responsibility to:
   a. 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).
   b. Ensure that all portable computing devices or personal computers in their custody are running industry recognized malicious software protection controls.
   c. Immediately report any suspected or actual incidence of malicious software infection as a security incident per IR-001-Security Incident Response.

## References

1. GP-001.02-Security Exceptions and Exemptions to ITS Standards and Practices
2. CS-001 Device Life Cycle Security
3. IR-001-Security Incident Response