Cyber Tree Systems
A Business IT Solution Company

Anti-Virus Policy

1.0 Statement of Purpose

The purpose of this policy is to provide guidance for utilizing anti-virus software and preventing the introduction of malicious software or access to CTS corporate-owned systems, where “corporate-owned” is defined as any system operating in a CTS production environment on the company network, whether within the company-owned facilities or issued to company agents or employees for use at remote locations for company business.

2.0 Scope

This policy applies to all CTS employees and affiliates.

3.0 Policy

3.1 General Guidelines

- Always run the corporate standard. Supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding; refer to CTS's Acceptable Use Policy.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette from an unknown source for viruses before using it. Back up critical data and system configurations on a regular basis and store the data in a safe place via a cloud-based service.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- Firewall-based Intrusion Prevention System (IPS) scanning will be implemented to detect and mitigate malware threats in real-time across network traffic.
- Any device connecting to the CTS enterprise network via VPN must comply with updated endpoint protection policies, ensuring they have the latest security patches, anti-virus updates, and malware detection mechanisms enabled.

3.2 Ownership

Responsibility will befall to IS/IT/InfoSec staff to verify current anti-virus revisions, maintain the corporate download website with current updates for corporate assets, and ensure firewall-based IPS scanning is operational.

4.0 Enforcement

Any employee found to be in violation this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Macro	In Microsoft Word and other programs, a macro is a saved sequence of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke.
Virus	A virus is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document.
Firewall-based IPS	A security system that monitors network traffic suspicious activities and takes automated
Endpoint Protection	Security Measures designed to ensure that all remote devices connecting to the corporate network comply with security policies and are protected against malware threats.

6.0 Revision History

Revision Number	Date	Editor	Reason
2.0	1/16/2025	Aidan Schmeckpeper	Separated into library and prepared for future edits.
2.1	2/19/2025	Aidan Schmeckpeper	Better conform to new organizational chart and firewall/VPN policy