Cyber Tree Systems
A Business IT Solution Company

Systems Management Policy

1.0 Purpose

The purpose of this policy is to provide guidelines for system management as implemented within the CTS network both within the network infrastructure, pertaining to workstations and server-class computers.

2.0 Scope

This policy applies to all CTS IS/IT employees.

3.0 Policy

3.1 Guidelines

3.1.1 Basic Client Computer Configuration Policy

All computer systems must be configured according to the NIST checklist to ensure patching against the common system vulnerabilities. All systems must receive Operating System updates from the local Software Update Server, as dictated by the development team to ensure continued functionality of company proprietary software packages.

3.1.2 Basic Server Computer Configuration Policy

All servers must be hardened against common system vulnerabilities using the NIST Guides and vendor security update announcements. The server infrastructure will receive updates via SUS to ensure thorough and consistent system configurations. There must be a minimum level of security controls installed on each server to protect the infrastructure. All server changes, updates, upgrades must be approved through the change proposal process and logged into a change management database with timestamps.

3.1.2 Basic Cloud Services Configuration Policy

All cloud services should be configured and maintained per the Cloud Services Policy.

3.1.3 Firewall & VPN Update and Patching Schedule

All firewall and VPN devices must follow a scheduled update and patching cycle to maintain system integrity and security. Security updates and patches must be applied no later than 30 days after release unless critical vulnerabilities necessitate immediate deployment. All changes must be reviewed and approved through the change management process before implementation.

3.1.4 Firewall & VPN Log Review Policy

Firewall and VPN logs must be reviewed on a weekly basis to identify potential security incidents, unauthorized access attempts, or unusual activity. Automated monitoring solutions should be implemented where possible to assist in anomaly detection. Any suspicious findings must be escalated to the security team for further investigation.

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

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