1.0 PURPOSE

This policy describes how the organization manages the configuration of technology systems, creating them and keeping them aligned with industry best practices for security. Baseline configurations for systems and system components include connectivity, operational, and communications aspects of systems. Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture.

2.0 SCOPE

This policy applies to all organization-owned computer systems that come into contact with the organization's sensitive data.

3.0 POLICY

3.1 Baseline Configuration (3.4.1)

Systems are aligned with security hardening standards that are consistent with industry best practices, such as those maintained by Microsoft for Windows operating systems. System configuration is tracked, inventoried, and maintained by a central system, and this system acts to track deviations from the standard configuration. Configuration standards are documented in a system setup procedure document.

Changes to the baseline configuration are analyzed for their security impact. Changes can only be implemented by authorized personnel. Baseline configurations employ the principle of least functionality, such as by limiting administrative functions only to authorized individuals. System components that are not needed for the routine functioning of devices are disabled.

3.2 Security Configuration Settings (3.4.2)

The following are enforced security settings for all in-scope systems used by the company:

- Regular user accounts do not have administrative abilities.
- Advanced endpoint protection software is installed and cannot be removed without administrative authorization.
- System security settings cannot be changed by the user without administrative authorization.

3.3 Configuration Change Control (3.4.3, 3.4.4, 3.4.5)

Changes to security configuration settings require administrative approval and must be tracked in an issue management system. Proposed changes must be evaluated for their security impact prior to implementation. Only authorized individuals may implement system changes.

3.4 Least Functionality (3.4.6, 3.4.7)

Systems are designed such that only required functionality is enabled. Advanced endpoint protection software acts to prevent unauthorized software from running. Non-privileged users are not authorized to install software on systems. Systems are regularly inventoried for installed software.

3.5 Application Control (3.4.8, 3.4.9)

Applications are monitored and controlled and blocked where necessary to protect system security. Users may not install unauthorized software on company systems.

4.0 RELEVANT NIST CONTROLS

Control	Control Description	Document Section
NIST 800-171 3.4	Baseline Configuration – All sections	Entire Document

5.0 REVISION HISTORY

Date	Name	Changes Made	Revision #
10/9/2023	Frank Schipani	Initial draft created	0.9
12/30/2023	Audit Committee	Approved Policies	