System and Information Integrity (SI) Policy

Document Version: 1.1

January 16, 2022

DoD Supply Company System and Information Integrity Policy

Last Updated: *January 2022*

1. Overview

System and Information Integrity (SI) practices are designed to identify and manage flaws that need remediation and monitoring for malicious code across DoD Supply Company systems, networks, and email. DoD Supply Company System and Info Integrity activities ensure that technology assets (e.g., desktops, software) that contain FCI are continuously monitored to detect violations of the authorized security state. Additionally, e-mail, a common attack vector, will be monitored and protected to detect malicious activity. The purpose of this policy is to provide guidelines for establishing System and Information Integrity practices for DoD Supply Company information systems and activities.

2. Purpose

The purpose of this policy is to secure and protect the information assets owned by DoD Supply Company Corporation. DoD Supply Company provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives to protect Federal Contract Information (FCI) and company proprietary information . DoD Supply Company grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

3. Scope

This policy applies to all of DoD Supply Company employees, contractors and vendors who connect to IT resources (e.g., workstations, servers, applications, or network devices) that contain or transmit DoD Supply Company information. This policy applies regardless of whether the access is to a local machine (i.e., DoD Supply Company-issued laptop or desktop computer) or a non-local resource, such as network-based file shares.

4. Roles and Responsibilities

Role	Responsibility
Executive Leadership	Approve and support the policy
CIO	Develop the policy and direct its adoption corporate wide
CISO	• Maintain the policy • Enforce compliance

Users	• Comply with the policy • Report any needed exceptions or non-compliance to the IT Manager

5. Guidelines and Regulations

5.1 CMMC

All activities related to the application of systems and information integrity principles must be in compliance with the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) version 2.0.

5.2 NIST 800-171 & FAR Clause 52.204-21

All activities related to the application of systems and information integrity principles must comply with the basic safeguarding requirements and procedures to protect covered contractor information systems in Federal Acquisition Regulation (FAR) Clause 52.204-21

All activities related to the application of systems and information integrity principles must also comply with the guidelines in the National Institute of Standards and Technology (NIST) Special Publication 800-171, Revision 2.

6. Policy

General Requirements

- The DoD Supply Company CIO shall develop and implement procedures to enforce strict System and Information Integrity measures across the enterprise.

6.1 Flaw Remediation (SI.L1-3.14.1)

- The DoD Supply Company IT Department will ensure the to protection the integrity of information systems within the network by employing the proper patch management and update techniques listed below:

    - Identify system flaws: full network scans will be completed, at minimum, every 48 hours. The IT team will ensure automated systems scan are configured and running properly
    - Reports of system scans with vulnerabilities will be **immediately** sent to the IT Manager for flaw remediation
    - Information system flaws will be remediated within 48 hours of any testing and analysis, if possible. Any extension to this time frame should be requested through the IT Manager.

6.1.1 Patch Management

The DoD Supply Company IT Department will conduct patching and updates in an expedient manner; however, the following practices will be utilized when applying critical security patches and/or bug fixes/featured updates:

- Use centralized patch management (Windows Server Update Service (WSUS))
- Install security-relevant software updates immediately upon their release on non-critical information systems
- Install security-relevant software updates after testing critical information systems
- Install any bugs fixes or feature updates after testing

6.2 Malicious Code Protection (SI.L1-3.14.2)

- The DoD Supply Company will utilize malicious code protection at the following inbound and outbound network traffic points and information systems:

  - ASA (DoD-SU-ASA-01)
  - Firewall (DoD-SU-FW-01)
  - All workstations
  - All servers

  The DoD Supply Company IT Department will products that automatically scan/protect information systems/network devices. In addition, all workstations and servers will be centrally configured and managed by Microsoft System Center Configuration Manager (SCCM) for application vulnerabilities.

6.2.1 Malicious Code Protection Procedures

DoD Supply Company IT Department malicious code protection practices and procedures are addressed in DoD-PRO-SI-314, which can be found at the following SharePoint link:

Intranet.dodsupplyco.com/sites/file-store/CMMC/Procedures/DoD-PRO-SI-314

6.3 Update Malicious Code Protection (SI.L1-3.14.4)

- The DoD Supply Company will update malicious code protection on all systems automatically daily. The following will be included in the processes outlined in DoD-PRO-SI-314:

  - Workstation antivirus/antimalware updates
  - Server antivirus/antimalware updates
  - Network appliance antivirus/antimalware updates

6.4 Update Malicious Code Protection (SI.L1-3.14.5)

- The DoD Supply Company IT Depart will perform periodic scans of all DoD Supply Company information systems and ensure real-time scans of files from external sources are performed on all user workstations, as well as other organizational endpoints as files are downloaded, opened, or executed. The following requirements for scans will be included in the processes outlined in DoD-PRO-SI-314:

    - Scanning of DoD Supply Company information systems:
        - Servers – every 24 hours
        - Workstations/endpoints – every 24 hours

    - Real-time scans will be configured and managed in Microsoft SCCM to ensure the following systems and user endpoints are scanned when downloading, opening, or executing files:

        - All Servers
        - HR Department
        - IT Department
        - Security Office
        - Warehouse

7. Policy Compliance

General Compliance

The IT Manager will develop and implement processes to ensure that this policy and any procedural guides are applied consistently to all aspects of physical security to ensure physical safeguards remain in place in all operating units.

8. Exceptions

Any exception to the policy must be documented and approved by the DoD Supply Company IT Manager.

9. Enforcement

The IT Manager and team will regularly perform manual and automated testing to ensure all systems are compliant with this policy.

10. Related Standards, Policies and Processes

- IT Security Policy
- DoD-PRO-SI-314

11. Revision History

The revision history shall be maintained throughout the entire life of this policy. Each published update shall be recorded. Full revisions (1.0) are considered a complete reissuance of the policy and are greater than or equal to 10% of the document. Partial revision (1.1) is considered minor corrections and don't require reissuance.

Revision History:

Version Number	Change criteria	Date
1.0	Initial document draft approval/release	09/11/21
1.1	Updates to correct CMMC v2.0 changes	1/16/22

12. Approval and endorsement by management

This policy is fully endorsed by all levels of the DoD Supply Company Management and Leadership Team, to include the company owner who is responsible for all contracts and associated customer, proprietary, and FCI data.

John Smith

John Smith
Owner, DoD Supply Company