Access Control (AC) Policy

Document Version: 1.3

January 16, 2022

Last Update Status: *Updated January 2022*

1. Overview

Access controls are designed to limit access to authorized users and personnel, thereby protecting corporate resources. Access Control is defined as the process of granting or denying specific requests to:

- obtain and use information and related information processing services; and
- enter specific physical facilities (e.g., company offices, plants and supporting facilities).

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 in order 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. Policy

General Requirements

- The DoD Supply Company CIO shall develop and implement procedures to enforce strict access control measures across the enterprise.
- These procedures should include and enforce the minimum requirements listed below:
  - All access to DoD Supply Company systems and data will be provided to users based on business requirements, job function, responsibilities, or need-to-know.
  - All modification to the standard access will require an Account Modification Request form to be completed and submitted to the Information Technology (IT) Department and must include:
    - a detailed business justification for the modified access;
    - the length of time that the modified access will be required;
    - written approval from the requestor's immediate supervisor; and
    - written approval from the group supervisor.

Privileged Accounts

- Access to and use of privileged accounts (e.g., local administrator, domain administrator, root, etc.) shall be restricted and controlled, and not provided by default.
- These accounts will require the written approval from the requestor's immediate supervisor, group supervisor and division director.
- These accounts are to be limited in use to only administrative functions. All functions that can be performed with a basic user account should not be performed with the administrate account (e.g., email use, web access, messaging, etc.)
- The maximum time for the expiration of all administrative accounts shall be no longer than 30 days.
- The following accounts are authorized privileged access to Company Proprietary and FCI data:

Name	Title	Highest System Access
John Smith	Information Owner	Domain Admin #2
William Smith	CISO	Domain Admin #1
Janis Overworked	SSO	Privileged User
Robert Technical	IT Manager	Privileged User
Michael Gethired	HR Supervisor	Privileged User

Processes Acting on behalf of users (Service Accounts)

- The following service accounts are authorized privileged access to Company Proprietary and FCI data:

Name	Owner	Highest System Access
sp19SvcApp.SA	Information Owner	Privileged User

Devices authorized

- The following devices are authorized to access to Company Proprietary and FCI data:

Computer/System	Owner	Computer/System	Owner
RHEL-SU-INV-01	Information Owner	DoD-SU-ASA-01	Information Owner
DoD-SU-DC-01	Information Owner	DoD-SU-RT-01	Information Owner
DoD-SU-SQL-01	Information Owner	DoD-SU-SW-01	Information Owner
WS-MAC-01	William Smith	DoD-SU-FW-01	Information Owner
WS-WIN-01	Janis Overworked		
WS-WIN-02	Michael Gethired		
WS-LIN-01	Robert Technical		
DoD-SU-PRT-01	Information Owner		

External Connections

- The following external systems access to the DoD Supply Company network and information systems is authorized:
    - Any external service provider listed below is/are required to connect vis MLPS or site-to-site (FIPS-140-2 validate) VPN.
        - Main DoD Supply Company
    - DoD Supply Company personnel connecting via mobile device are only authorized to do so after completing a Mobile Device Authorization Request. All personnel will access the DoD Supply Company network and information systems with an organization provided and managed device. No personal, BYOD[1], devices are authorized.

Note: 1- Bring your own device (BYOD) refers to the trend of employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data

Mobile Device Authorization

- The following mobile devices are authorized to access to Company Proprietary and FCI data:

Computer/System	Device Type	Owner
DoD-SU-MD-01	Cell Phone	John Smith
DoD-SU-MD-02	Cell Phone	William Smith
DoD-SU-MD-03	Cell Phone	Janis Overworked
DoD-SU-MD-04	Cell Phone	Robert Technical
DoD-SU-MD-05	Cell Phone	Michael Gethired
DoD-SU-MD-06	iPad	Janis Overworked

Control Public Information

- **Request for Release of Information to the Public**

- DoD Supply Company will control information posted or processed on publicly accessible information systems. The only personnel authorized to post or processes information on a publicly accessible information system is the Information Owner. All information to be posted on the DoD Supply Company public website or social media sites will first be screen by the HR Supervisor and then sent to the Information Manager for a second review and posting. For procures on posting information see the **DoD Supply Company Public Media Release Procedure and Form**.

- **Improper posting of proprietary or FCI data (removal)**

  DoD Supply Company will immediately remove any connect that has accidentally been placed on social media and/or the companies public facing website. The HR Supervisor and/or IT Manager will follow the procedures outline in the **DoD Supply Company Public Media Removal Procedures**. The website hosting agent listed in the procedures should be contacted per the outlined timelines in the procedures.

6. Policy Compliance

- **General Compliance**

The IT department will develop and implement a process to ensure that this policy and any procedural guides are applied consistently to all systems throughout all operating units.

7. Exceptions

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

Enforcement

The Infosec team will develop a process and procedures to regularly perform manual and automated testing to ensure all systems are compliant with this policy. Related Standards, Policies and Processes

- IT Security Policy
- IT Security Procedures
- Procedures

8. 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	12/20/21
1.1	Corrected IT Department titles	1/9/22
1.2	Added Public information control procedure link	1/10/22
1.3	Updates to correct grammatical errors	1/16/22

9. 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 the government contract and (FCI) data.

John Smith

John Smith
Owner, DoD Supply Company