Identification and Authentication (IA) Policy

Document Version: 1.2

January 16, 2022

DoD Supply Company Identification and Authentication Policy

Last Updated: *January 2022*

1. Overview

Identification and Authentication practices are designed to identify information system users, processes acting on behalf of users, or devices. The purpose of this policy is to provide guidelines for establishing identification and authentication practices for DoD Supply Company information systems.

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 Identification and Authentication 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 access control requirements in conjunction with the identification and authentication practices listed below.
  - All modification to the standard identification and authentication methods 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 identification and authentication;
    - the length of time that the modification to identification and authentication will be required;
    - written approval from the requestor's immediate supervisor; and
    - written approval from the group supervisor.

Identification (IA.L1-3.5.1)

- System administrators will assign individual, unique identifiers (e.g., usernames) to all users, processes, and devices that access DoD Supply Company information systems.
- These unique identifiers will consist of a short set of alphanumeric characters that refer to the organizational component or personnel they represent (e.g., SW-0l would represent a network switch, SW-02 could refer to a different network switch). Below are the requirements for usernames, processes, and devices within the DoD Supply Company enterprise:

Devices:

Organizational Name	Unique Identifier
Switch	DoD-SU-SW-01
Router	DoD-SU-RT-01
Firewall	DoD-SU-FW-01
Adaptive Security Appliance (ASA)	DoD-SU-ASA-01
Windows Workstation	DoD-SU-WIN-01
Mac Workstations	DoD-SU-MAC-01
Linux Workstations	DoD-SU-LIN-01
Mobile Device	DoD-SU-MD-01
Windows Server (to included suite/build #)	DoD-SU-(Role)-01 DoD-SU-DC-01
Linux Server (to included suite/build #)	DISTRO-SVR-(Role)-(01) RHEL-SVR-INV-01

User Accounts and Processes:

Organizational Name	Unique Identifier
Service Account	ServiceAccountName.SA@ SQLSrvAccount.SA@dodsupplyco.com
Standard User Account	(first initial).(last name)@ j.doe@dodsupplyco.com
Privileged User Account	(first initial).(last name).priv@ j.doe.priv@dodsupplyco.com
Administrator Account	(first initial).(last name).priv@ j.smith.admin@dodsupplyco.com
Domain Administrator Account	(first initial).(last name).priv@ j.smith.DA@dodsupplyco.com

Authentication (IA.L1-3.5.2)

- Individual, unique passwords will be used by all DoD Supply Company information systems users and processes acting on behalf of users; devices will utilize MAC Address, trusted platform modules (TPM) or certificate-based authentication for access to FCI information systems and networks.
- The below criteria are the minimum authentication standards for network and system access to FCI data:

Organizational Identity	Authentication Method
Workstations, Laptops, Servers, Mobile Devices, IoT Devices	MAC Address, trusted platform module (TPM) or X.509 certificates
Standard User Account	10 or more characters long Must be alphanumeric with (2) symbols
Privileged User Account	14 or more characters long Must be alphanumeric with (4) symbols
Service Accounts/ Processes Acting on Behalf of User Accounts	14 or more characters long Must be alphanumeric with (4) symbols
Administrator Account	14 or more characters long Must be alphanumeric with (4) symbols
Domain Administrator Account	16 or more characters long Must be alphanumeric with (6) symbols

Note: example symbols are !,@,#,$,%

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.

8. Related Standards, Policies and Processes

- IT Security Policy
- IT Security Procedures

9. 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	Updates to correct grammatical errors	1/16/22

10. 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