Alpha Nine Fabrication, Inc.
Controlled Unclassified Information (CUI)

Document ID: ANF-POL-AC-001

Title: Access Control Policy

Version: 1.0

Effective Date: 2025-11-08

Approved By: Chief Information Security Officer (CISO)

ACCESS CONTROL POLICY (ANF-POL-AC-001)

1. Purpose

The purpose of this Access Control Policy is to define the principles and requirements governing authorization, access, and management of information systems that process, store, or transmit Controlled Unclassified Information (CUI) within Alpha Nine Fabrication, Inc. (ANF). This policy ensures compliance with NIST SP 800-171 Rev 2 and CMMC Level 2 requirements.

2. Scope

This policy applies to all personnel, contractors, consultants, vendors, and systems within ANF's network zones (SECBUS, CADCAM, SHOPFLOOR, OIT, SECOPS, and CORP) that access or manage CUI data.

3. Roles and Responsibilities

• Chief Information Security Officer (CISO): Approves and enforces this policy and oversees access control compliance.

• SECOPS Manager: Implements technical controls for authentication, authorization, and access monitoring.

• OIT Manager: Manages account provisioning, deactivation, and system access configurations.

• Department Managers: Validate user access requests and review access rights quarterly.

• All Users: Comply with all access policies and immediately report unauthorized access attempts.

4. Policy Statement

Access to ANF systems shall be granted based on the principles of least privilege, need-to-know, and role-based access control (RBAC). All users and devices must be uniquely identified, authenticated, and authorized prior to system access. Access rights shall be regularly reviewed and promptly revoked when no longer required.

5. Key Policy Areas

• User Access Authorization – All access requests require documented approval through the account provisioning workflow (PROC-AC-P01).

• Privileged Access Management – Elevated accounts shall be limited, time-bound, and monitored through security logging.

• Separation of Duties – System administration, audit review, and security operations duties shall be assigned to different personnel where feasible.

• Remote Access – Remote connections to CUI systems must comply with the Remote Access Standard (STD-AC-002).

• Wireless Access – Wireless access to CUI networks must use WPA3-Enterprise encryption with 802.1X authentication.

• Access Review – Department heads shall perform quarterly access reviews and submit results to SECOPS for validation.

• Account Revocation – Access shall be terminated within 24 hours of employee separation or role change.

6. Enforcement

Violations of this policy may result in disciplinary action up to and including termination of employment, loss of system access privileges, or legal action as appropriate. System monitoring and audits will be used to ensure compliance.

7. References

• NIST SP 800-171 Rev 2, Control Family 3.1 – Access Control

• NIST SP 800-53 Rev 5, Access Control (AC) Controls

• CMMC Model, Level 2 Requirements

APPROVALS

_____ _____

Chief Information Security Officer (CISO) Date

_____ _____

Vice President, OIT / CIO Date

_____ _____

Chief Executive Officer (CEO) Date