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

Document ID: ANF-STD-AC-002

Title: Remote Access Standard

Version: 1.0

Effective Date: 2025-11-08

Approved By: Chief Information Security Officer (CISO)

REMOTE ACCESS STANDARD (STD-AC-002)

1. Purpose

The purpose of this Remote Access Standard is to define secure methods for connecting to Alpha Nine Fabrication, Inc. (ANF) information systems from remote locations, ensuring the confidentiality, integrity, and availability of Controlled Unclassified Information (CUI).

2. Scope

This standard applies to all employees, contractors, and vendors who require remote access to ANF systems within SECBUS, CADCAM, SHOPFLOOR, OIT, SECOPS, or CORP network zones. It applies to all remote access technologies including VPN, SSH, RDP, and cloud-based interfaces.

3. Roles and Responsibilities

• CISO: Approves remote access technologies and ensures compliance with federal cybersecurity requirements.

• SECOPS Manager: Implements and monitors all remote access controls and VPN configurations.

• OIT Manager: Administers user accounts, VPN gateways, and device compliance enforcement.

• End Users: Comply with this standard and maintain security of remote devices and credentials.

4. Approved Remote Access Methods

• Secure Virtual Private Network (VPN) using IPSec with AES-256 encryption.

Copyright – Compliance Automation Engineering LLC
All rights reserved – January 2, 2026

• Azure Virtual Desktop or Remote Desktop Gateway with TLS 1.3 encryption.

• Secure Shell (SSH) or SFTP using public key authentication (RSA-4096 or ECC-P384).

• HTTPS/TLS-protected web applications hosted in the Azure Government Cloud.

5. Authentication Requirements

• Multifactor Authentication (MFA) is mandatory for all remote sessions.

• AD-based credentials must comply with password and complexity policies (see PROC-AC-P01).

• Device authentication must be validated through NAC before establishing connection.

• Service accounts used for automation must use key-based authentication with restricted privileges.

6. Encryption Requirements

All remote access connections must employ end-to-end encryption using FIPS 140-3 validated cryptographic modules. The following encryption standards apply:

• Data in transit: TLS 1.3, IPSec, SSH (AES-256 or ChaCha20-Poly1305).

• Authentication: RSA-4096 or ECC-P384 certificates managed by Azure Key Vault.

• Management interfaces: HTTPS only; Telnet and unencrypted FTP are prohibited.

7. Session Management

• All remote sessions shall automatically terminate after 30 minutes of inactivity.
• Concurrent remote sessions from the same account are prohibited.
• VPN clients must force all traffic through the corporate gateway (no split tunneling).
• System logs must record user ID, source IP, time of connection, and duration.

8. Prohibited Technologies

The following remote access methods are strictly prohibited due to security risks:
• Unencrypted RDP or Telnet sessions
• Consumer VPNs or public proxy services
• Remote access from public or unsecured Wi-Fi networks without VPN
• File transfer via personal cloud storage (Google Drive, Dropbox, etc.)

Copyright – Compliance Automation Engineering LLC
All rights reserved – January 2, 2026

9. Monitoring and Enforcement

All remote access activity shall be continuously monitored by SECOPS via SIEM and Azure Sentinel. Non-compliance with this standard may result in disciplinary action, revocation of remote access privileges, or further administrative or legal action.

10. References

- POL-AC-001 – Access Control Policy
- PROC-AC-P01 – Account Provisioning Procedure
- NIST SP 800-171 Rev 2, Controls 3.1.12 through 3.1.16 – Remote Access and Encryption
- CMMC Level 2 – Access Control (AC) Requirements

APPROVALS

_____ _____

Chief Information Security Officer (CISO) Date

_____ _____

Vice President, OIT / CIO Date

_____ _____

Chief Executive Officer (CEO) Date

Alpha Nine Fabrication, Inc. – Controlled Unclassified Information (CUI) – Do Not Distribute Without Authorization.

Copyright – Compliance Automation Engineering LLC
All rights reserved – January 2, 2026