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

Document ID: SOP-DEVSECOPS-CICD-001

Title: Secure CI/CD and Release Management Procedure

Version: 1.0

Effective Date: 2025-11-09

Approved By: Chief Information Security Officer (CISO)

SECURE CI/CD AND RELEASE MANAGEMENT PROCEDURE (SOP-DEVSECOPS-CICD-001)

1. Purpose

This procedure defines the secure software development, integration, testing, and deployment practices implemented within Alpha Nine Fabrication, Inc. (ANF) to ensure compliance with NIST SP 800-171 Rev 2, CMMC Level 2, and internal cybersecurity policies. It establishes the process for maintaining confidentiality, integrity, and availability of Controlled Unclassified Information (CUI) throughout the software lifecycle via a secured GitLab DevSecOps pipeline.

2. Scope

This procedure applies to all applications, automation, and infrastructure code repositories maintained within ANF's GitLab instance and deployed into environments supporting the SECBUS, CADCAM, SHOPFLOOR, OIT, SECOPS, and CORP network zones. It covers all DevSecOps processes involving CI/CD pipelines, approvals, scanning, and release management.

3. Roles and Responsibilities

• Developers: Implement secure code, run local tests, and submit merge requests for review. Developers cannot directly deploy to production.

• DevSecOps Engineer: Maintains pipeline configurations, GitLab runners, and scanning integrations.

• SECOPS Manager: Reviews vulnerabilities and oversees enforcement of CI/CD security gates.

• OIT Manager: Approves releases for deployment and manages production environments.

• CISO: Approves this SOP, ensures compliance with CMMC Level 2, and validates audit readiness.

4. CI/CD Workflow Overview

• Validate – Code linting, syntax validation, and dependency version checks.

• Build – Application or container image creation using secure base images from ANF's internal registry.

• Test – Automated unit and integration testing with results stored as artifacts.

• SAST – Automated code scanning for vulnerabilities and coding flaws.

• Secret and Dependency Scanning – Detects credentials, API keys, and insecure library dependencies.

• Container and IaC Scanning – Ensures images and infrastructure definitions meet CIS and DISA STIG compliance baselines.

• DAST – Executes runtime vulnerability scanning against test environments.

• SBOM Generation – Produces a CycloneDX-compliant Software Bill of Materials (SBOM) for supply chain integrity.

• Stage Deployment – Automated deployment to staging with verification and SECOPS validation.

• Production Approval – Manual approval step by SECOPS and OIT ensures separation of duties before release.

• Production Deployment – Controlled, logged release to production systems using protected GitLab runners.

5. Control Mapping Table

CI/CD Function	NIST SP 800-171 Rev 2 Controls	CMMC Level 2 Capability	Supporting ANF Documents
Access Restrictions / RBAC	3.1.1, 3.1.2, 3.1.5	AC.1.001, AC.2.005	POL-AC-001, PROC-AC-P01
Change Approval / Separation of Duties	3.1.4, 3.4.5	AC.2.007, CM.2.064	POL-AC-001, SOP-DEVSECOPS-CICD-001
Audit Logging and Review	3.3.1, 3.3.2, 3.3.3	AU.2.042, AU.3.045	CA-RPT-2025, Risk Register
Code Integrity /	3.4.1, 3.4.2	CM.2.061	PROC-AC-P01

Build Verification			
Vulnerability Scanning (SAST, DAST, IaC)	3.14.1, 3.14.2	SI.2.216, SI.2.217	SOP-SI-001, SI-LOG-2025
SBOM Generation / Supply Chain Assurance	3.13.1, 3.13.3	SC.3.177, SC.3.180	SOP-SC-002, SC-ARCH-2025
Manual Approval Gate for Production	3.1.5, 3.1.6	AC.2.007	POL-AC-001, PROC-AC-P01
Pipeline Audit Evidence Retention	3.12.1, 3.12.3	CA.2.158, CA.2.159	CA-RPT-2025, POA&M Database
Incident Logging and Monitoring	3.6.1, 3.6.2	IR.2.093	POL-IR-001, IR-LOG-2025
Continuous Monitoring / Risk Updates	3.11.1, 3.11.2	RA.2.142	POL-RA-001, Risk Register

---

APPROVALS

_____ _____

Chief Information Security Officer (CISO) Date

_____ _____

Vice President, OIT / CIO Date

_____ _____

Chief Executive Officer (CEO) Date