Northgate Defense Systems, LLC	Document ID	CMMC-POL-001
	Version	1.0
Federal Contract Information	Effective Date	March 1, 2026
	Document Owner	Rachel Okafor
	Approved By	David Whitfield

Table of Contents

1. Introduction and Purpose

1.1 Introduction

This Federal Contract Information (FCI) Protection Policy establishes the security framework for Northgate Defense Systems, LLC to protect Federal Contract Information in accordance with the Federal Acquisition Regulation (FAR) Clause 52.204-21 and the Cybersecurity Maturity Model Certification (CMMC) 2.0 Level 1 requirements. This policy serves as the master security policy governing all activities related to the handling, processing, storage, and transmission of FCI within the organization's information systems.

As a contractor or subcontractor within the Defense Industrial Base (DIB), Northgate Defense Systems, LLC is entrusted with Federal Contract Information that, while not classified, requires protection from unauthorized disclosure and access. The Department of Defense has implemented the CMMC program to verify that contractors are meeting their contractual obligations to protect FCI and, where applicable, Controlled Unclassified Information (CUI).

CMMC Level 1 focuses on the protection of FCI through the implementation of 17 basic safeguarding practices derived from FAR 52.204-21. These practices represent fundamental cybersecurity hygiene that all contractors handling FCI must implement and maintain. This policy establishes the governance framework and security requirements necessary to achieve and maintain CMMC Level 1 compliance.

Compliance with this policy and the underlying CMMC Level 1 requirements is mandatory for contract eligibility with the Department of Defense. Beginning with the CMMC Acquisition Rule effective November 2025, contractors must demonstrate compliance through annual self-assessment and affirmation in the Supplier Performance Risk System (SPRS) as a condition of contract award.

1.2 Purpose

The purpose of this policy is to establish the security governance framework for protecting Federal Contract Information and achieving CMMC Level 1 compliance. Specifically, this policy aims to:

- Define the requirements for identifying, handling, and protecting Federal Contract Information throughout its lifecycle within Northgate Defense Systems, LLC's information systems and business processes.
- Establish the implementation requirements for all 17 CMMC Level 1 practices across the six security domains: Access Control, Identification and Authentication, Media Protection, Physical Protection, System and Communications Protection, and System and Information Integrity.
- Define roles and responsibilities for CMMC compliance, including the designation of a Senior Company Official responsible for attesting to the organization's compliance status.
- Establish the framework for conducting annual self-assessments, maintaining evidence of compliance, documenting any gaps through Plans of Action and Milestones (POA&M), and submitting required information to SPRS.
- Ensure that Northgate Defense Systems, LLC maintains eligibility for Department of Defense contracts by demonstrating compliance with FAR 52.204-21 and CMMC Level 1 requirements.
- Protect Northgate Defense Systems, LLC from False Claims Act liability by establishing documented policies, procedures, and evidence of compliance with contractual cybersecurity obligations.

1.3 Policy Statement

Northgate Defense Systems, LLC is committed to protecting Federal Contract Information entrusted to us by the Department of Defense and prime contractors. We recognize that the protection of FCI is both a contractual obligation and a matter of national security interest.

All personnel who access, handle, process, store, or transmit Federal Contract Information shall comply with this policy and the supporting procedures, standards, and guidelines that implement CMMC Level 1 requirements. No exceptions to these requirements shall be permitted without formal approval through the exception process defined in this policy.

The organization shall maintain a CMMC Level 1 compliance posture at all times. This includes conducting annual self-assessments, promptly addressing any identified gaps, maintaining current evidence of compliance, and submitting accurate affirmations to SPRS. The Senior Company Official shall personally affirm the organization's compliance status, understanding that false attestation carries significant legal consequences under the False Claims Act.

Northgate Defense Systems, LLC shall implement all 17 CMMC Level 1 practices as specified in this policy and supporting documentation. These practices shall be integrated into normal business operations and maintained as standard operating procedures rather than treated as one-time compliance activities.

1.4 Regulatory Foundation

This policy is based on and implements the following regulatory requirements:

Regulation/Standard	Description
FAR 52.204-21	Basic Safeguarding of Covered Contractor Information Systems - establishes 15 security requirements (mapping to 17 CMMC practices) for protecting FCI
32 CFR Part 170	CMMC Program Rule - establishes the CMMC framework, assessment requirements, and certification levels
CMMC Model v2.0	Defines the 17 Level 1 practices across 6 domains derived from FAR 52.204-21
NIST SP 800-171 Rev 2	Source of the security requirements that CMMC Level 1 practices map to (subset)
NIST SP 800-171A	Assessment procedures and objectives used to evaluate CMMC Level 1 practice implementation
48 CFR Part 204	CMMC Acquisition Rule - incorporates CMMC requirements into DoD contracts

2. Scope

2.1 Organizational Scope

This policy applies to Northgate Defense Systems, LLC and all business units, divisions, departments, and locations that process, store, or transmit Federal Contract Information in connection with Department of Defense contracts or subcontracts.

The policy applies to the CMMC Assessment Scope, which includes all assets that process, store, or transmit FCI. The organization may achieve CMMC Level 1 for its entire enterprise

network or for a defined enclave, depending on where FCI is handled. The boundaries of the assessment scope shall be documented and maintained.

2.2 Personnel Scope

This policy applies to all individuals who may access Federal Contract Information or systems that process FCI, including:

- Employees at all levels who work on or support DoD contracts.
- Contractors, consultants, and temporary workers with access to FCI or FCI systems.
- Subcontractors who receive FCI flow-down from Northgate Defense Systems, LLC.
- Any other individuals granted access to systems within the CMMC Assessment Scope.

2.3 Systems Scope

This policy applies to all information systems and technology assets within the CMMC Assessment Scope that process, store, or transmit Federal Contract Information.

This includes:

- Workstations, laptops, and other endpoint devices used to access or process FCI.
- Servers and infrastructure that store or process FCI.
- Network infrastructure that transmits FCI.
- Cloud services and applications used for FCI processing.
- Mobile devices that access FCI systems.
- Physical facilities where FCI systems are located or FCI is handled.

Specialized assets such as government-furnished equipment, IoT devices, and operational technology are assessed separately as specified in CMMC scoping guidance.

2.4 Information Scope

This policy applies to all Federal Contract Information as defined by FAR 52.204-21. FCI is information not intended for public release that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. FCI does not include:

- Information provided by the Government to the public.
- Simple transactional information necessary to process payments.
- Controlled Unclassified Information (CUI), which requires CMMC Level 2 protection.

The organization shall maintain an inventory of FCI types and the systems that process them to ensure appropriate protection measures are applied.

3. Definitions

Term	Definition
Federal Contract Information (FCI)	Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, excluding information provided to the public

	or simple transactional information for payment processing.
Covered Contractor Information System	An unclassified information system that is owned or operated by a contractor and that processes, stores, or transmits Federal Contract Information.
CMMC Assessment Scope	The set of all assets that will be assessed against CMMC practices. For Level 1, this includes assets that process, store, or transmit FCI.
Senior Company Official	An individual within the organization who has the authority to ensure the organization's compliance with CMMC requirements and to affirm the accuracy of assessment results.
Supplier Performance Risk System (SPRS)	The DoD's authoritative source for contractor performance and risk assessment information where CMMC self-assessment results and affirmations are recorded.
Plan of Action and Milestones (POA&M)	A document that identifies tasks to be accomplished to address security weaknesses, the resources required, milestones for completion, and scheduled completion dates.
Practice	A CMMC security requirement that must be implemented. CMMC Level 1 contains 17 practices across 6 domains.
Domain	A grouping of related CMMC practices. Level 1 practices are organized into 6 domains: AC, IA, MP, PE, SC, and SI.
Self-Assessment	An evaluation conducted by the organization itself to determine compliance with CMMC Level 1 requirements, following the assessment objectives in NIST SP 800-171A.
Affirmation	A formal attestation by the Senior Company Official confirming the organization's continued compliance with CMMC requirements.

4. Federal Contract Information Requirements

4.1 FCI Identification

Northgate Defense Systems, LLC shall establish and maintain processes to identify Federal Contract Information throughout its lifecycle. All personnel working on DoD contracts shall be trained to recognize FCI and understand their obligations for its protection.

FCI identification shall occur at the following points:

- Contract award and task order initiation, when FCI types are identified in contract requirements.
- Receipt of information from the Government or prime contractors.
- Creation of information in performance of contract requirements.
- Communication and collaboration with Government personnel or other contractors.

The organization shall maintain documentation of FCI types handled and the systems used to process them. This documentation supports the definition of the CMMC Assessment Scope and ensures appropriate protections are applied.

4.2 FCI Handling

Federal Contract Information shall be handled in accordance with the following requirements:

- FCI shall only be processed, stored, or transmitted on systems within the defined CMMC Assessment Scope that implement all required Level 1 practices.
- FCI shall not be stored on personal devices, personal cloud storage, or systems outside the assessment scope unless specifically authorized and protected.
- FCI shall be protected from unauthorized access through implementation of access controls, authentication, and physical protection measures.
- FCI shall be disposed of securely when no longer needed, using approved sanitization or destruction methods.
- FCI shared with subcontractors shall include appropriate flow-down of protection requirements.

4.3 FCI Marking

While FAR 52.204-21 does not mandate specific marking requirements for FCI, Northgate Defense Systems, LLC shall implement internal practices to identify and track FCI:

- Electronic files containing FCI should include identification in the filename, header, or metadata where practical.
- Physical documents containing FCI should be marked to indicate they require protection.
- Systems and storage locations containing FCI should be identified to personnel.
- Marking practices shall be documented and communicated to personnel who handle FCI.

5. CMMC Level 1 Security Requirements

Northgate Defense Systems, LLC shall implement all 17 CMMC Level 1 practices as specified below. Each practice shall be fully implemented; partial implementation does not satisfy the requirement. Supporting policies, procedures, and evidence templates are provided in the CMMC Level 1 Compliance Kit.

5.1 Access Control (AC)

The Access Control domain ensures that only authorized users, processes, and devices can access FCI systems and that their actions are appropriately limited.

AC.L1-3.1.1 — Authorized Access Control

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Implementation: The organization shall maintain a list of authorized users for each system containing FCI. Access shall only be granted to individuals with a legitimate business need. Accounts shall be created, modified, and terminated through a formal process with appropriate approvals. Devices connecting to FCI systems shall be identified and authorized.

AC.L1-3.1.2 — Transaction and Function Control

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Implementation: The organization shall implement role-based or function-based access controls that limit users to only those transactions and functions required for their job responsibilities. Administrative privileges shall be restricted to personnel requiring them. Users shall not have access to functions beyond their assigned role.

AC.L1-3.1.20 — External Connections

Verify and control/limit connections to and use of external information systems.

Implementation: The organization shall identify and document all connections between FCI systems and external systems. Connections shall be authorized, monitored, and controlled through firewalls and boundary protection devices. Access to external systems from within the FCI environment shall be restricted to authorized business purposes.

AC.L1-3.1.22 — Public Information Control

Control information posted or processed on publicly accessible information systems.

Implementation: The organization shall establish procedures to review information before posting to publicly accessible systems to ensure FCI is not inadvertently disclosed. Personnel authorized to post public content shall be identified. Public-facing systems shall be reviewed periodically to verify no FCI has been posted.

5.2 Identification and Authentication (IA)

The Identification and Authentication domain ensures that users, processes, and devices are properly identified and authenticated before accessing FCI systems.

IA.L1-3.5.1 — Identification

Identify information system users, processes acting on behalf of users, or devices.

Implementation: The organization shall assign unique identifiers to all users who access FCI systems. Shared accounts shall not be used except where technically unavoidable and documented. Devices shall be uniquely identifiable. Processes acting on behalf of users shall be associated with the authorizing user.

IA.L1-3.5.2 — Authentication

Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Implementation: The organization shall require authentication before granting access to FCI systems. Passwords shall meet minimum complexity requirements. Default passwords shall be changed before systems are put into production. Authentication mechanisms shall verify claimed identity before granting access.

5.3 Media Protection (MP)

The Media Protection domain ensures that FCI stored on media is protected from unauthorized disclosure during disposal or reuse.

MP.L1-3.8.3 — Media Disposal

Sanitise or destroy information system media containing Federal Contract Information before disposal or release for reuse.

Implementation: The organization shall sanitize or destroy all media containing FCI before disposal or transfer outside the organization. Approved sanitization methods include secure overwriting, degaussing, or physical destruction depending on media type. Sanitization and destruction shall be documented, including date, method, and responsible individual.

5.4 Physical Protection (PE)

The Physical Protection domain ensures that FCI systems and the facilities housing them are protected from unauthorized physical access.

PE.L1-3.10.1 — Physical Access Limitation

Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

Implementation: The organization shall restrict physical access to facilities and areas containing FCI systems to authorized personnel. Access control mechanisms such as locks, badges, or guards shall be implemented. Areas containing FCI systems shall be identified and access appropriately restricted.

PE.L1-3.10.3 — Visitor Escort and Monitoring

Escort visitors and monitor visitor activity.

Implementation: Visitors to areas containing FCI systems shall be escorted by authorized personnel at all times. Visitor activity shall be monitored to prevent unauthorized access to FCI or systems. Visitors shall not be left unattended in areas containing FCI systems.

PE.L1-3.10.4 — Physical Access Logs

Maintain audit logs of physical access.

Implementation: The organization shall maintain logs of physical access to facilities and areas containing FCI systems. Logs shall include identity of individual, date, time, and area accessed. Logs shall be retained for a period sufficient to support security reviews and incident investigation.

PE.L1-3.10.5 — Physical Access Devices

Control and manage physical access devices.

Implementation: The organization shall control physical access devices such as keys, badges, and access cards. An inventory of access devices and their assignment shall be maintained. Lost or stolen devices shall be reported and deactivated promptly. Access devices shall be recovered when personnel no longer require access.

5.5 System and Communications Protection (SC)

The System and Communications Protection domain ensures that communications containing FCI are monitored and protected at system boundaries.

SC.L1-3.13.1 — Boundary Protection

Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

Implementation: The organization shall implement boundary protection mechanisms such as firewalls at external network boundaries. Communications crossing boundaries shall be monitored and controlled. Internal boundaries between FCI systems and other systems shall be protected where applicable.

SC.L1-3.13.5 — Public Access System Separation

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Implementation: Publicly accessible system components such as web servers shall be placed in a separate network segment (DMZ) from internal systems containing FCI. Logical or physical separation shall prevent direct access from public systems to internal FCI systems.

5.6 System and Information Integrity (SI)

The System and Information Integrity domain ensures that system flaws are identified and corrected and that malicious code is detected and eradicated.

SI.L1-3.14.1 — Flaw Remediation

Identify, report, and correct information and information system flaws in a timely manner.

Implementation: The organization shall implement a process to identify system flaws and vulnerabilities. Security patches and updates shall be applied in a timely manner based on severity. A patch management process shall track identification, testing, and deployment of updates.

SI.L1-3.14.2 — Malware Protection

Provide protection from malicious code at appropriate locations within organizational information systems.

Implementation: The organization shall deploy anti-malware solutions on systems within the FCI assessment scope. Anti-malware protection shall be deployed at appropriate locations including endpoints, servers, and network boundaries. Protection shall be configured to detect and respond to malicious code.

SI.L1-3.14.4 — Malware Protection Updates

Update malicious code protection mechanisms when new releases are available.

Implementation: The organization shall configure anti-malware solutions to receive automatic updates. Signature and engine updates shall be applied promptly when available. Update status shall be monitored to ensure systems remain current.

SI.L1-3.14.5 — System and File Scanning

Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Implementation: The organization shall configure anti-malware solutions to perform real-time scanning of files from external sources. Periodic full-system scans shall be scheduled and executed. Scan results shall be reviewed and detected threats addressed promptly.

6. Self-Assessment and Affirmation

6.1 Annual Self-Assessment

Northgate Defense Systems, LLC shall conduct an annual self-assessment of its implementation of CMMC Level 1 practices. The self-assessment shall evaluate each of the 17 practices against the assessment objectives defined in NIST SP 800-171A.

The self-assessment shall:

- Evaluate all 17 practices using appropriate assessment methods: examine, interview, and test.
- Document evidence of implementation for each practice.
- Identify any practices that are not fully implemented.
- Calculate the overall compliance status (all practices must be MET for Level 1).
- Document findings in a remediation plan. As CMMC Level 1 does not permit a Plan of Action and Milestones (POA&M) for certification, all identified gaps must be fully remediated (closed) prior to SPRS submission.

Self-assessments shall be conducted using the CMMC-ASSESS-001 Self-Assessment Workbook provided in this kit.

6.2 SPRS Submission

Following completion of the self-assessment and remediation of any gaps, Northgate Defense Systems, LLC shall submit the results to the Supplier Performance Risk System (SPRS).

The submission shall include:

- The date of the self-assessment.
- The scope of systems assessed.
- The overall assessment result (all 17 practices must be MET).
- Confirmation that no practices are in POA&M status (CMMC Level 1 requires full implementation).

SPRS submissions shall be updated following each annual self-assessment or when significant changes occur to the compliance status.

6.3 Senior Official Affirmation

In addition to the annual self-assessment, the designated Senior Company Official shall provide an annual affirmation attesting to the organization's continued compliance with CMMC Level 1 requirements.

The Senior Company Official:

- Shall be an individual with authority to ensure the organization's compliance with CMMC requirements.
- Shall review the self-assessment results before providing affirmation.
- Shall understand that the affirmation is a legally binding statement subject to False Claims Act penalties if inaccurate.
- Shall affirm continued compliance annually, or confirm that remediation is in progress if gaps exist.

6.4 Continuous Compliance

Northgate Defense Systems, LLC shall maintain CMMC Level 1 compliance continuously, not only at the time of assessment.

This requires:

- Ongoing implementation of all 17 practices as standard operating procedures.
- Regular monitoring to ensure practices remain effective.

- Prompt remediation of any identified gaps or deficiencies.
- Updating documentation and evidence as systems and processes change.
- Re-assessment when significant changes occur to systems, processes, or the FCI environment.

7. Roles and Responsibilities

7.1 Senior Company Official

The Senior Company Official is the individual designated to oversee CMMC compliance and provide attestation of the organization's compliance status.

Responsibilities include:

- Ensuring the organization allocates adequate resources for CMMC compliance.
- Reviewing and approving the FCI Protection Policy and supporting documentation.
- Reviewing self-assessment results and approving SPRS submissions.
- Providing annual affirmation of continued compliance to SPRS.
- Understanding the legal implications of affirmation under the False Claims Act.
- Ensuring prompt remediation of identified compliance gaps.
- The Senior Company Official for Northgate Defense Systems, LLC is: Rachel Okafor, CISO.

7.2 CMMC Program Manager

The CMMC Program Manager is responsible for the day-to-day management of the CMMC compliance program.

Responsibilities include:

- Maintaining this policy and supporting documentation.
- Coordinating annual self-assessments and evidence collection.
- Managing the POA&M and tracking remediation activities.
- Preparing SPRS submissions for Senior Official review.
- Providing guidance to personnel on CMMC requirements.
- Coordinating training and awareness activities related to FCI protection.
- Reporting compliance status to the Senior Company Official.
- The CMMC Program Manager for Northgate Defense Systems, LLC is: Rachel Okafor, CISO.

7.3 IT/Security Personnel

IT and Security personnel are responsible for implementing and maintaining the technical controls required by CMMC Level 1.

Responsibilities include:

- Implementing access controls, authentication, and boundary protection.
- Managing user accounts and access permissions.
- Maintaining anti-malware and patch management systems.

- Monitoring systems for security events and anomalies.
- Performing media sanitization and destruction.
- Maintaining documentation of system configurations and security controls.
- Supporting self-assessment activities and providing evidence of implementation.

7.4 All Personnel

All personnel who access FCI or systems within the CMMC Assessment Scope are responsible for:

- Complying with this policy and supporting procedures.
- Protecting their credentials and not sharing passwords.
- Reporting suspected security incidents or policy violations.
- Completing required security awareness training.
- Handling FCI appropriately and only on authorized systems.
- Escorting visitors and protecting physical access to FCI areas.
- Cooperating with self-assessment and audit activities.

8. Compliance and Enforcement

8.1 Compliance Requirements

Compliance with this policy and CMMC Level 1 requirements is mandatory for all personnel within scope.

Compliance is verified through:

- Annual self-assessments against CMMC Level 1 practices.
- Ongoing monitoring of security controls and practices.
- Review of evidence documentation.
- Potential Government review of SPRS submissions and supporting documentation.

All 17 CMMC Level 1 practices must be fully implemented (MET status) for the organization to claim Level 1 compliance. Unlike higher CMMC levels, Level 1 does not allow for conditional certification with a POA&M.

8.2 Violations and Consequences

Violations of this policy may result in disciplinary action commensurate with the severity of the violation, including:

- Verbal or written warnings.
- Required additional training.
- Revocation of access to FCI systems.
- Termination of employment or contract.
- Referral for legal action in cases of intentional misconduct.

Violations that result in unauthorized disclosure of FCI may also trigger notification obligations under the contract and could affect the organization's eligibility for future contracts.

8.3 False Claims Act Liability

Northgate Defense Systems, LLC and its personnel must understand the serious legal consequences of inaccurate compliance claims. The False Claims Act (31 U.S.C. § 3729) imposes significant penalties on contractors who knowingly submit false claims to the Government, including:

- Civil penalties of up to $11,000 per false claim.
- Treble damages (three times the Government's loss).
- Potential criminal prosecution for fraud.
- Debarment from future Government contracts.

Submitting a CMMC self-assessment or affirmation that inaccurately represents the organization's compliance status may constitute a false claim. The Senior Company Official and others involved in compliance attestation must ensure that all submissions are accurate and supported by documented evidence.

9. Related Documents

This policy is supported by the following documents within the CMMC Level 1 Compliance Kit:

Document ID	Document Title	Purpose
CMMC-POL-002	Access Control Policy	AC domain practices
CMMC-POL-003	Identification and Authentication Policy	IA domain practices
CMMC-POL-004	Media Protection Policy	MP domain practices
CMMC-POL-005	Physical Protection Policy	PE domain practices
CMMC-POL-006	System and Communications Protection Policy	SC domain practices
CMMC-POL-007	System and Information Integrity Policy	SI domain practices
CMMC-PROC-001 to 006	Supporting Procedures	Operational implementation
CMMC-FRM-001 to 010	Forms and Evidence Templates	Evidence documentation
CMMC-ASSESS-001	Self-Assessment Workbook	Annual assessment
CMMC-ASSESS-002	SPRS Score Calculator	SPRS submission
CMMC-GUIDE-001	Getting Started Guide	Implementation roadmap
CMMC-GUIDE-002	FCI Identification Guide	FCI scoping
CMMC-GUIDE-	Evidence Requirements Guide	Assessment preparation

003		

10. Policy Exceptions

Exceptions to this policy are strongly discouraged given the contractual and legal requirements for CMMC Level 1 compliance. However, in rare circumstances where a specific practice cannot be implemented as specified, exceptions may be considered.

Exception requests shall:

- Document the specific practice for which an exception is requested.
- Explain why full implementation is not feasible.
- Describe compensating controls that provide equivalent protection.
- Include risk assessment of the exception.
- Specify the duration and conditions of the exception.

Exceptions must be approved by the Senior Company Official after review by the CMMC Program Manager. Approved exceptions shall be documented and factored into the self-assessment process. Note that exceptions may affect the organization's ability to claim full CMMC Level 1 compliance.

Any exception shall be reviewed when circumstances change and shall not exceed one year without re-approval.

11. Document Control

11.1 Document Information

Document Title	Federal Contract Information Protection Policy
Document ID	CMMC-POL-001
Version	1.0
Classification	Internal Use
Effective Date	March 1, 2026
Next Review Date	March 1, 2027
Document Owner	Rachel Okafor, CISO
Approved By	David Whitfield, Chief Executive
Regulatory Basis	FAR 52.204-21, 32 CFR Part 170, CMMC Model v2.0

11.2 Revision History

Version	Date	Author	Description of Changes
0.1	March 1, 2026	Information Security Team	Initial draft
0.2	March 1, 2026	Information Security Team	Incorporated review feedback

1.0	March 1, 2026	Information Security Team	Approved for release

11.3 Approval Signatures

Role	Name	Signature	Date
Senior Company Official	Rachel Okafor		
CMMC Program Manager	Rachel Okafor		
IT/Security Manager	Rachel Okafor		

Disclaimer

This document is provided as a customizable template for organizations seeking to establish CMMC Level 1 compliance. It is intended to be adapted to each organization's specific circumstances, systems, and business processes.

This document does not constitute legal advice. While it is based on publicly available regulatory requirements including FAR 52.204-21 and the CMMC Program Rule (32 CFR Part 170), organizations are responsible for ensuring their compliance approach meets all applicable requirements.

Organizations should consult with qualified legal counsel and cybersecurity professionals to ensure their compliance program is appropriate for their specific situation. The accuracy of CMMC self-assessments and affirmations is the responsibility of the organization and its designated Senior Company Official.

RidgeLine Cyber Defence provides this template in good faith but makes no warranty regarding its suitability for any particular purpose or its compliance with any specific regulatory requirement.