RIDGELINE CYBER DEFENCE

CMMC Level 1 Compliance Kit

Complete documentation package for CMMC Level 1 self-assessment. Covers all 17 practices across 6 domains with policies, procedures, and evidence templates.

DOCUMENTS	FRAMEWORKS	FORMAT
35+	CMMC 2.0, NIST SP 800-171, CSF 2.0	Word (.docx) + Excel (.xlsx)

PRODUCT PREVIEW

This document provides a preview of the product contents, structure, and sample documentation quality. Visit ridgelinecyber.com to purchase the full toolkit.

WHAT'S INCLUDED

The CMMC Level 1 Compliance Kit contains the following documents, templates, and tools:

Domain Policies (6 Documents)

- Access Control (AC) Domain Policy
- Identification and Authentication (IA) Domain Policy
- Media Protection (MP) Domain Policy
- Physical Protection (PE) Domain Policy
- System and Communications Protection (SC) Domain Policy
- System and Information Integrity (SI) Domain Policy

Practice-Level Procedures (17 Documents)

- AC.L1-3.1.1 Authorised Access Control Procedure
- AC.L1-3.1.2 Transaction and Function Control Procedure
- AC.L1-3.1.20 External Connections Control Procedure
- AC.L1-3.1.22 Public Information Control Procedure
- IA.L1-3.5.1 User Identification Procedure
- IA.L1-3.5.2 Authentication Procedure
- MP.L1-3.8.3 Media Sanitisation Procedure
- PE.L1-3.10.1 Physical Access Limitation Procedure
- PE.L1-3.10.3 Escort Visitors Procedure
- PE.L1-3.10.4 Physical Access Logs Procedure
- PE.L1-3.10.5 Physical Access Control Procedure
- SC.L1-3.13.1 Boundary Protection Procedure
- SC.L1-3.13.5 Public Access System Separation Procedure
- SI.L1-3.14.1 Flaw Remediation Procedure
- SI.L1-3.14.2 Malicious Code Protection Procedure
- SI.L1-3.14.4 Update Malicious Code Protection Procedure
- SI.L1-3.14.5 System and File Scanning Procedure

Self-Assessment Tools

- CMMC Level 1 Self-Assessment Workbook (Excel)
- SPRS Score Calculator
- System Security Plan (SSP) Template
- Plan of Action and Milestones (POA&M;) Template
- Evidence Collection Checklist (by Practice)
- Assessment Readiness Review Checklist

Supporting Documentation

- CUI Scope and Boundary Definition Guide
- Assessor Preparation Guide
- Quick Start Implementation Guide

- CMMC to NIST CSF 2.0 Cross-Mapping Reference

Access Control Domain Policy

Document ID: CMMC-AC-POL-001 | Version: 1.0 | Classification: Internal | Status: Template

1. Purpose

This policy establishes the access control requirements for [Organisation Name] to protect Federal Contract Information (FCI) in accordance with CMMC Level 1 requirements. It addresses practices AC.L1-3.1.1, AC.L1-3.1.2, AC.L1-3.1.20, and AC.L1-3.1.22, ensuring that access to information systems and data is limited to authorised users, processes, and devices, and is restricted to authorised transactions and functions.

2. Scope

This policy applies to all information systems, networks, and data repositories that process, store, or transmit Federal Contract Information (FCI) within the defined CMMC assessment boundary. All personnel, contractors, and third parties with access to FCI-handling systems are subject to this policy.

3. Policy Requirements

3.1 Authorised Access Control (AC.L1-3.1.1): Access to organisational information systems shall be limited to authorised users, processes acting on behalf of authorised users, and authorised devices. All access shall be based on approved business requirements and shall be formally authorised prior to granting access. 3.2 Transaction and Function Control (AC.L1-3.1.2): Access to information systems shall be limited to the types of transactions and functions that authorised users are permitted to execute. Role-based access controls shall be implemented to enforce least privilege principles. 3.3 External Connections (AC.L1-3.1.20): Connections to external information systems shall be verified and controlled. All external connections shall be approved, documented, and monitored.

This is a preview excerpt. The full document continues with additional sections including detailed implementation requirements, roles and responsibilities, compliance measures, exceptions process, and review procedures.

FRAMEWORK CROSS-MAPPING EXAMPLE

Every document in the toolkit includes framework traceability. Below is an example of how our documentation maps to multiple compliance frameworks simultaneously.

NIST CSF 2.0	ISO 27001:2022	CIS Controls v8	RidgeLine Document
PR.AA-05	A.5.15	AC.L1-3.1.1	Access Control Domain Policy
PR.AA-03	A.8.5	IA.L1-3.5.2	Authentication Procedure
PR.DS-01	A.7.10	MP.L1-3.8.3	Media Sanitisation Procedure
PR.AA-06	A.7.1, A.7.2	PE.L1-3.10.1	Physical Access Limitation
PR.IR-01	A.8.20	SC.L1-3.13.1	Boundary Protection Procedure
PR.PS-02	A.8.8	SI.L1-3.14.1	Flaw Remediation Procedure

Ready to close your governance gaps?

The full CMMC Level 1 Compliance Kit includes every document shown in this preview — plus all supporting standards, procedures, forms, templates, and cross-mapping workbooks.

Starting from $249

ridgelinecyber.com/cmmc-compliance-kit/

contact@ridgelinecyber.com

14-day money-back guarantee | Instant download | Customise and deploy in days

This is a customisable template product only. It is not legal advice. Organisations should seek qualified professional advice for their specific circumstances and jurisdiction.