YourIT!
Your Logo Goes Here

CMMC 2.0 - Level 1

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

Purpose

The purpose is to ensure that qualifying defense contractors and subcontractors meet all the requirements defined in DFARS and FAR contractual obligations and associated guidance.

Scope

This policy applies to the workforce members of defense contractors or subcontractors that access, process, or store Federal Contract Information (FCI). This policy also applies to service providers and security vendors who provide IT management, cybersecurity services, or security tools.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

CMMC 2.0 AC.L1-3.1.1 - Limit System Access

CMMC 2.0 - Level 1	Other Requirements
AC.L1-3.1.1 Limit System Access	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
This requirement focuses on account management for systems and applications. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement AC.L1-3.1.2. Identify users, processes, and devices that are allowed to use company computers and can log on to the company network. Automated updates and other automatic processes should be associated with the user who initiated (authorized) the process. Limit the devices (e.g., printers) that can be accessed by company computers. Set up your system so that only authorized users, processes, and devices can access the company network.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.11 - Access Termination: Implement procedures for terminating access when the employment of a workforce member ends or as required by other determinations.
- CC7.12 - Limit Access: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 AC.L1-3.1.2 - Limit Transactions & Functions

CMMC 2.0 - Level 1	Other Requirements
AC.L1-3.1.2 Limit Transactions & Functions	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of origin. In defining other account attributes, organizations consider system-related requirements (e.g., system upgrades scheduled maintenance,) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.9 - Workforce Authorization & Supervision: Implement procedures for the authorization and/or supervision of workforce members.
- CC7.13 - Limit Functions: Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 AC.L1-3.1.20 - External Connections

CMMC 2.0 - Level 1	Other Requirements
AC.L1-3.1.20 External Connections	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include vendor and personally owned systems, components, or devices and privately-owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of CUI, including accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems. Organizations establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum, the types of applications that can be accessed on organizational systems from external systems. If terms and conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems. This requirement recognizes that there are circumstances where individuals using external systems (e.g., contractors, coalition partners) need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been effectively implemented can be achieved by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations. Note that while "external" typically refers to outside of the organization's direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. And among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered "external" to that system.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.10 - Appropriate Access: Implement procedures to determine that the access of a workforce member is appropriate.
- CC7.14 - Control External Information Systems: Verify and control/limit connections to and use of external information systems.

References

- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 AC.L1-3.1.22 - Control Public Information

CMMC 2.0 - Level 1	Other Requirements
AC.L1-3.1.22 Control Public Information	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Control information posted or processed on publicly accessible information systems.

Guidance
Common device identifiers include media access control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device. NIST SP 800-63-3 provides guidance on digital identities.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.15 - Control Publicly Accessible Systems: Control information posted or processed on publicly accessible information systems.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 IA.L1-3.5.1 - Identification

CMMC 2.0 - Level 1	Other Requirements
IA.L1-3.5.1 Identification	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
Common device identifiers include media access control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device. NIST SP 800-63-3 provides guidance on digital identities.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.7 - Unique User Identification: Assign a unique name and/or number for identifying and tracking user identity.
- CC7.16 - Identify System Users: Identify information system users, processes acting on behalf of users, or devices.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 IA.L1-3.5.2 - Authentication

CMMC 2.0 - Level 1	Other Requirements
IA.L1-3.5.2 Authentication	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
Individual authenticators include the following: passwords, key cards, cryptographic devices, and one-time password devices. Initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include the minimum password length. Developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include certificates and passwords.

NIST SP 800-63-3 provides guidance on digital identities.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.8 - Identity Authentication: Implement procedures to verify that a person or entity seeking access to data is the one claimed.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 MP.L1-3.8.3 - Media Disposal

CMMC 2.0 - Level 1	Other Requirements
MP.L1-3.8.3 Media Disposal	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
This requirement applies to all system media, digital and non-digital, subject to or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or . Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization.

Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or . Sanitization of non-digital media includes destruction, removing FCI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for federal contract information. NIST SP 800-88 provides guidance on media sanitization.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC8.24 - Disposal: Implement policies and procedures to address the final disposition of electronic data and/or the hardware or electronic media on which it is stored.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 PE.L1-3.10.1 - Limit Physical Access

CMMC 2.0 - Level 1	Other Requirements
PE.L1-3.10.1 Limit Physical Access	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
This requirement applies to employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials that include badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.2 - Physical Access Management: Manage and protect physical access to assets.
- CC11.2 - Control Physical Access: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control.
- CC11.5 - Restrict Physical Access: Implement physical safeguards for all workstations and operating environments to restrict access to authorized users.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 PE.L1-3.10.3 - Escort Visitors

CMMC 2.0 - Level 1	Other Requirements
PE.L1-3.10.3 Escort Visitors	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Escort visitors and monitor visitor activity.

Guidance
Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.17 - Escort & Monitor Visitors: Escort visitors and monitor visitor activity.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 PE.L1-3.10.4 - Physical Access Logs

CMMC 2.0 - Level 1	Other Requirements
PE.L1-3.10.4 Physical Access Logs	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Maintain audit logs of physical access.

Guidance
Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., written log of individuals accessing the facility), automated (e.g. capturing ID provided by a Personal Identity Verification (PIV) card), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. System components (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.20 - Physical Access Logs: Maintain audit logs of physical access.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 PE.L1-3.10.5 - Manage Physical Access

CMMC 2.0 - Level 1	Other Requirements
PE.L1-3.10.5 Manage Physical Access	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Control and manage physical access devices.

Guidance
Physical access devices include keys, locks, combinations, and card readers.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC7.19 - Physical Access Devices: Control and manage physical access devices.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 SC.L1-3.13.1 - Boundary Protection

CMMC 2.0 - Level 1	Other Requirements
SC.L1-3.13.1 Boundary Protection	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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.

Guidance
Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes restricting external web communications traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. NIST SP 800-41 provides guidance on firewalls and firewall policy. NIST SP 800-125B provides guidance on security for virtualization technologies.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC13.5 - Monitor, Control, and Protect Communications: 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.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 SC.L1-3.13.5 - Public-Access System Separation

CMMC 2.0 - Level 1	Other Requirements
SC.L1-3.13.5 Public-Access System Separation	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloud• based technologies.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC13.6 - Implement Subnetworks: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 SI.L1-3.14.1 - Flaw Remediation

CMMC 2.0 - Level 1	Other Requirements
SI.L1-3.14.1 Flaw Remediation	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation. NIST SP 800-40 provides guidance on patch management technologies.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC8.18 - Install Patches & Updates: Ensure that all software and firmware are updated with patches and updates within 7 days of becoming available, unless warnings indicate a faster implementation is required.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

CMMC 2.0 SI.L1-3.14.2 - Malicious Code Protection

CMMC 2.0 - Level 1	Other Requirements
SI.L1-3.14.2 Malicious Code Protection	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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

Guidance
Designated locations include system entry and exit points which may include firewalls, remote access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities. Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. [SP 800-83] provides guidance on malware incident prevention.
Training users to recognize and avoid suspicious emails and files is an effective supplement to technical tools to protect against malicious code.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CC8.19 - Firewall Protection: Ensure that firewalls with active intrusion prevention protect the perimeter of the network.
- CC8.20 - Malicious Software Protection & Detection: Implement procedures for guarding against, detecting, and reporting malicious software.
- CC18.12 - Malicious Code Detection: Ensure that malicious code is detected.

References
- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html

- CMMC 2.0 Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC 2.0 Level 1 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_Final_20211210.pdf

Truncated Sample Report