

CMMC 2.0 - Level 2

Policies and Procedures



CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Table of Contents

01	Purpose
02	Scope
03	Sanctions/Compliance
04	CMMC 2.0 AC.L1-3.1.1 - Limit System Access
05	CMMC 2.0 AC.L1-3.1.2 - Limit Transactions & Functions
06	CMMC 2.0 AC.L1-3.1.20 - External Connections
07	CMMC 2.0 AC.L1-3.1.22 - Control Public Information
08	CMMC 2.0 AC.L2-3.1.10 - Session Lock
09	CMMC 2.0 AC.L2-3.1.11 - Session Termination
10	CMMC 2.0 AC.L2-3.1.12 - Control Remote Access
11	CMMC 2.0 AC.L2-3.1.13 - Remote Access Confidentiality
12	CMMC 2.0 AC.L2-3.1.14 - Remote Access Routing
13	CMMC 2.0 AC.L2-3.1.15 - Privileged Remote Access
14	CMMC 2.0 AC.L2-3.1.16 - Wireless Access Authorization
15	CMMC 2.0 AC.L2-3.1.17 - Wireless Access Protection
16	CMMC 2.0 AC.L2-3.1.18 - Mobile Device Connection
17	CMMC 2.0 AC.L2-3.1.19 - Encrypt CUI on Mobile
18	CMMC 2.0 AC.L2-3.1.21 - Portable Storage Use
19	CMMC 2.0 AC.L2-3.1.3 - Control CUI Flow
20	CMMC 2.0 AC.L2-3.1.4 - Separation of Duties
21	CMMC 2.0 AC.L2-3.1.5 - Least Privilege
22	CMMC 2.0 AC.L2-3.1.6 - Non-Privileged Account Use
23	CMMC 2.0 AC.L2-3.1.7 - Privileged Functions
24	CMMC 2.0 AC.L2-3.1.8 - Unsuccessful Logon Attempts
25	CMMC 2.0 AC.L2-3.1.9 - Privacy & Security Notices
26	CMMC 2.0 AT.L2-3.2.1 - Role-Based Risk Awareness
27	CMMC 2.0 AT.L2-3.2.2 - Role-Based Training
28	CMMC 2.0 AT.L2-3.2.3 - Insider Threat Awareness
29	CMMC 2.0 AU.L2-3.3.1 - System Auditing

30	CMMC 2.0 AU.L2-3.3.2 - User Accountability
31	CMMC 2.0 AU.L2-3.3.3 - Event Review
32	CMMC 2.0 AU.L2-3.3.4 - Audit Failure Alerting
33	CMMC 2.0 AU.L2-3.3.5 - Audit Correlation
34	CMMC 2.0 AU.L2-3.3.6 - Reduction & Reporting
35	CMMC 2.0 AU.L2-3.3.7 - Authoritative Time Source
36	CMMC 2.0 AU.L2-3.3.8 - Audit Protection
37	CMMC 2.0 AU.L2-3.3.9 - Audit Management
38	CMMC 2.0 CA.L2-3.12.1 - Security Control Assessment
39	CMMC 2.0 CA.L2-3.12.2 - Plan of Action
40	CMMC 2.0 CA.L2-3.12.3 - Security Control Monitoring
41	CMMC 2.0 CA.L2-3.12.4 - System Security Plan
42	CMMC 2.0 CM.L2-3.4.1 - System Baselineing
43	CMMC 2.0 CM.L2-3.4.2 - Security Configuration Enforcement
44	CMMC 2.0 CM.L2-3.4.3 - System Change Management
45	CMMC 2.0 CM.L2-3.4.4 - Security Impact Analysis
46	CMMC 2.0 CM.L2-3.4.5 - Access Restrictions for Change
47	CMMC 2.0 CM.L2-3.4.6 - Least Functionality
48	CMMC 2.0 CM.L2-3.4.7 - Nonessential Functionality
49	CMMC 2.0 CM.L2-3.4.8 - Application Execution Policy
50	CMMC 2.0 CM.L2-3.4.9 - User-Installed Software
51	CMMC 2.0 IA.L1-3.5.1 - Identification
52	CMMC 2.0 IA.L1-3.5.2 - Authentication
53	CMMC 2.0 IA.L2-3.5.10 - Cryptographically-Protected Passwords
54	CMMC 2.0 IA.L2-3.5.11 - Obscure Feedback
55	CMMC 2.0 IA.L2-3.5.3 - Multifactor Authentication
56	CMMC 2.0 IA.L2-3.5.4 - Replay-Resistant Authentication
57	CMMC 2.0 IA.L2-3.5.5 - Identifier Reuse
58	CMMC 2.0 IA.L2-3.5.6 - Identifier Handling
59	CMMC 2.0 IA.L2-3.5.7 - Password Complexity
60	CMMC 2.0 IA.L2-3.5.8 - Password Reuse
61	CMMC 2.0 IA.L2-3.5.9 - Temporary Passwords

62	CMMC 2.0 IR.L2-3.6.1 - Incident Handling
63	CMMC 2.0 IR.L2-3.6.2 - Incident Reporting
64	CMMC 2.0 IR.L2-3.6.3 - Incident Response Testing
65	CMMC 2.0 MA.L2-3.7.1 - Perform Maintenance
66	CMMC 2.0 MA.L2-3.7.2 - System Maintenance Control
67	CMMC 2.0 MA.L2-3.7.3 - Equipment Sanitization
68	CMMC 2.0 MA.L2-3.7.4 - Media Inspection
69	CMMC 2.0 MA.L2-3.7.5 - Nonlocal Maintenance
70	CMMC 2.0 MA.L2-3.7.6 - Maintenance Personnel
71	CMMC 2.0 MP.L1-3.8.3 - Media Disposal
72	CMMC 2.0 MP.L2-3.8.1 - Media Protection
73	CMMC 2.0 MP.L2-3.8.2 - Media Access
74	CMMC 2.0 MP.L2-3.8.4 - Media Markings
75	CMMC 2.0 MP.L2-3.8.5 - Media Accountability
76	CMMC 2.0 MP.L2-3.8.6 - Portable Storage Encryption
77	CMMC 2.0 MP.L2-3.8.7 - Removable Media
78	CMMC 2.0 MP.L2-3.8.8 - Shared Media
79	CMMC 2.0 MP.L2-3.8.9 - Protect Backups
80	CMMC 2.0 PE.L1-3.10.1 - Limit Physical Access
81	CMMC 2.0 PE.L1-3.10.3 - Escort Visitors
82	CMMC 2.0 PE.L1-3.10.4 - Physical Access Logs
83	CMMC 2.0 PE.L1-3.10.5 - Manage Physical Access Devices
84	CMMC 2.0 PE.L2-3.10.2 - Monitor Facility
85	CMMC 2.0 PE.L2-3.10.6 - Alternative Work Sites
86	CMMC 2.0 PS.L2-3.9.1 - Screen Individuals
87	CMMC 2.0 PS.L2-3.9.2 - Personnel Actions
88	CMMC 2.0 RA.L2-3.11.1 - Risk Assessments
89	CMMC 2.0 RA.L2-3.11.2 - Vulnerability Scan
90	CMMC 2.0 RA.L2-3.11.3 - Vulnerability Remediation
91	CMMC 2.0 SC.L1-3.13.1 - Boundary Protection
92	CMMC 2.0 SC.L1-3.13.5 - Public-Access System Separation
93	CMMC 2.0 SC.L2-3.13.10 - Key Management

94	CMMC 2.0 SC.L2-3.13.11 - CUI Encryption
95	CMMC 2.0 SC.L2-3.13.12 - Collaborative Device Control
96	CMMC 2.0 SC.L2-3.13.13 - Mobile Code
97	CMMC 2.0 SC.L2-3.13.14 - Voice over Internet Protocol
98	CMMC 2.0 SC.L2-3.13.15 - Communications Authenticity
99	CMMC 2.0 SC.L2-3.13.16 - Data at Rest
100	CMMC 2.0 SC.L2-3.13.2 - Security Engineering
101	CMMC 2.0 SC.L2-3.13.3 - Role Separation
102	CMMC 2.0 SC.L2-3.13.4 - Shared Resource Control
103	CMMC 2.0 SC.L2-3.13.6 - Network Communication by Exception
104	CMMC 2.0 SC.L2-3.13.7 - Split Tunneling
105	CMMC 2.0 SC.L2-3.13.8 - Data in Transit
106	CMMC 2.0 SC.L2-3.13.9 - Connections Termination
107	CMMC 2.0 SI.L1-3.14.1 - Flaw Remediation
108	CMMC 2.0 SI.L1-3.14.2 - Malicious Code Protection
109	CMMC 2.0 SI.L1-3.14.4 - Update Malicious Code Protection
110	CMMC 2.0 SI.L1-3.14.5 - System & File Scanning
111	CMMC 2.0 SI.L2-3.14.3 - Security Alerts & Advisories
112	CMMC 2.0 SI.L2-3.14.6 - Monitor Communications for Attacks
113	CMMC 2.0 SI.L2-3.14.7 - Identify Unauthorized Use

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 Controlled Unclassified Information (CUI) and 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 2 AC.L1-3.1.1 Limit System Access	Other Requirements 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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

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

CMMC 2.0 - Level 2 AC.L1-3.1.2 Limit Transactions & Functions	Other Requirements 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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

CMMC 2.0 AC.L1-3.1.20 - External Connections

CMMC 2.0 - Level 2 AC.L1-3.1.20 External Connections	Other Requirements 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

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 2 Assessment Guide -
https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

CMMC 2.0 AC.L1-3.1.22 - Control Public Information

CMMC 2.0 - Level 2 AC.L1-3.1.22 Control Public Information	Other Requirements 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

In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, FCI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post FCI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.

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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

CMMC 2.0 AC.L2-3.1.10 - Session Lock

<p>CMMC 2.0 - Level 2</p> <p>AC.L2-3.1.10</p> <p>Session Lock</p>	<p>Other Requirements</p> <p>N/A</p>
--	---

Policy

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

Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

Guidance

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday.

Pattern-hiding displays can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey controlled unclassified information.

Responsibilities

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

Related Internal Controls

- CC13.13 - Session Lock: Use session lock with pattern-hiding displays to prevent access/viewing of data after a period of inactivity.

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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

CMMC 2.0 AC.L2-3.1.11 - Session Termination

<p>CMMC 2.0 - Level 2</p> <p>AC.L2-3.1.11</p> <p>Session Termination</p>	<p>Other Requirements</p> <p>N/A</p>
---	---

Policy

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

Terminate (automatically) user sessions after a defined condition.

Guidance

This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.

Responsibilities

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

Related Internal Controls

- CC7.30 - Terminate Sessions: Terminate (automatically) user sessions after a defined condition.
- CC8.26 - Terminate Sessions: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

CMMC 2.0 AC.L2-3.1.12 - Control Remote Access

<p>CMMC 2.0 - Level 2</p> <p>AC.L2-3.1.12</p> <p>Control Remote Access</p>	<p>Other Requirements</p> <p>N/A</p>
---	---

Policy

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

Monitor and control remote access sessions.

Guidance

Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code.

Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing

connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

NIST SP 800-46, SP 800-77, and SP 800-113 provide guidance on secure remote access and virtual private networks.

Responsibilities

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

Related Internal Controls

- CC7.3 - Remote Access Management: Manage remote access to assets.

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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

CMMC 2.0 AC.L2-3.1.13 - Remote Access Confidentiality

CMMC 2.0 - Level 2 AC.L2-3.1.13 Remote Access Confidentiality	Other Requirements N/A
--	----------------------------------

Policy

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

Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

Guidance

Cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography.

Responsibilities

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

Related Internal Controls

- CC7.33 - Encrypt Remote Sessions: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

CMMC 2.0 AC.L2-3.1.14 - Remote Access Routing

CMMC 2.0 - Level 2 AC.L2-3.1.14 Remote Access Routing	Other Requirements N/A
--	----------------------------------

Policy

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

Route remote access via managed access control points.

Guidance

Routing remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.

Responsibilities

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

Related Internal Controls

- CC7.27 - Manage Remote Access: Route remote access via managed access control points.

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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

CMMC 2.0 AC.L2-3.1.15 - Privileged Remote Access

CMMC 2.0 - Level 2 AC.L2-3.1.15 Privileged Remote Access	Other Requirements N/A
---	----------------------------------

Policy

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

Authorize remote execution of privileged commands and remote access to security-relevant information.

Guidance

A privileged command is a human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. Security-relevant information is any information within the system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions. Controlling such access from remote locations helps to ensure that unauthorized individuals are not able to execute such commands freely with the potential to do serious or catastrophic damage to organizational systems. Note that the ability to affect the integrity of the system is considered security-relevant as that could enable the means to bypass security functions although not directly impacting the function itself.

Responsibilities

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

Related Internal Controls

- CC7.34 - Authorize Privileged Remote Sessions: Authorize remote execution of privileged commands and remote access to security-relevant information.

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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

CMMC 2.0 AC.L2-3.1.16 - Wireless Access Authorization

CMMC 2.0 - Level 2 AC.L2-3.1.16 Wireless Access Authorization	Other Requirements N/A
--	----------------------------------

Policy

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

Authorize wireless access prior to allowing such connections.

Guidance

Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols that provide credential protection and mutual authentication.

Responsibilities

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

Related Internal Controls

- CC7.25 - Authorize Wireless Access: Authorize wireless access prior to allowing such connections.

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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

CMMC 2.0 AC.L2-3.1.17 - Wireless Access Protection

CMMC 2.0 - Level 2 AC.L2-3.1.17 Wireless Access Protection	Other Requirements N/A
---	----------------------------------

Policy

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

Protect wireless access using authentication and encryption.

Guidance

Organizations authenticate individuals and devices to help protect wireless access to the system. Special attention is given to the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems.

Responsibilities

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

Related Internal Controls

- CC7.31 - Wireless Authentication & Encryption: Protect wireless access using authentication and encryption.

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 2 Assessment Guide - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

Truncated Sample Report