CMMC 2.0 AC.L1-3.1.20 - External Connections

CMMC 2.0 - Level 2	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

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_20211016_508.pdf

CMMC 2.0 AC.L1-3.1.22 - Control Public Information

CMMC 2.0 - Level 2	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
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_20211201 6_508.pdf

CMMC 2.0 AC.L2-3.1.10 - Session Lock

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

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_20211016_508.pdf

CMMC 2.0 AC.L2-3.1.11 - Session Termination

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

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_20211201 6_508.pdf

CMMC 2.0 AC.L2-3.1.12 - Control Remote Access

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

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_20211016_508.pdf

CMMC 2.0 AC.L2-3.1.13 - Remote Access Confidentiality

CMMC 2.0 - Level 2	Other Requirements
AC.L2-3.1.13 Remote Access Confidentiality	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_20211016_508.pdf

CMMC 2.0 AC.L2-3.1.14 - Remote Access Routing

CMMC 2.0 - Level 2	Other Requirements
AC.L2-3.1.14 Remote Access Routing	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_20211016_508.pdf

CMMC 2.0 AC.L2-3.1.15 - Privileged Remote Access

CMMC 2.0 - Level 2	Other Requirements
AC.L2-3.1.15 Privileged Remote Access	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 by-pass 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_20211016_508.pdf

CMMC 2.0 AC.L2-3.1.16 - Wireless Access Authorization

CMMC 2.0 - Level 2	Other Requirements
AC.L2-3.1.16 Wireless Access Authorization	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_20211016_508.pdf

CMMC 2.0 AC.L2-3.1.17 - Wireless Access Protection

CMMC 2.0 - Level 2	Other Requirements
AC.L2-3.1.17 Wireless Access Protection	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_20211016_508.pdf

Truncated Sample Report