YourIT!
Your Logo Goes Here

CMMC 2.13 - Level 2

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

Table of Contents

30	AU.L2-3.3.2 - User accountability
31	AU.L2-3.3.3 - Event review
32	AU.L2-3.3.4 - Audit failure alerting
33	AU.L2-3.3.5 - Audit correlation
34	AU.L2-3.3.6 - Reduction & reporting
35	AU.L2-3.3.7 - Authoritative time source
36	AU.L2-3.3.8 - Audit protection
37	AU.L2-3.3.9 - Audit management
38	CA.L2-3.12.1 - Security control assessment
39	CA.L2-3.12.2 - Operational plan of action
40	CA.L2-3.12.3 - Security control monitoring
41	CA.L2-3.12.4 - System security plan
42	CM.L2-3.4.1 - System baselining
43	CM.L2-3.4.2 - Security configuration enforcement
44	CM.L2-3.4.3 - System change management
45	CM.L2-3.4.4 - Security impact analysis
46	CM.L2-3.4.5 - Access restrictions for change
47	CM.L2-3.4.6 - Least functionality
48	CM.L2-3.4.7 - Nonessential functionality
49	CM.L2-3.4.8 - Application execution policy
50	CM.L2-3.4.9 - User-installed software
51	IA.L2-3.5.1 - Identification [CUI Data]
52	IA.L2-3.5.2 - Authentication [CUI Data]
53	IA.L2-3.5.3 - Multifactor authentication
54	IA.L2-3.5.4 - Replay-resistant authentication
55	IA.L2-3.5.5 - Identifier reuse
56	IA.L2-3.5.6 - Identifier handling
57	IA.L2-3.5.7 - Password complexity
58	IA.L2-3.5.8 - Password reuse
59	IA.L2-3.5.9 - Temporary passwords
60	IA.L2-3.5.10 - Cryptographically-protected passwords
61	IA.L2-3.5.11 - Obscure feedback

62	IR.L2-3.6.1 - Incident handling
63	IR.L2-3.6.2 - Incident reporting
64	IR.L2-3.6.3 - Incident response testing
65	MA.L2-3.7.1 - Perform maintenance
66	MA.L2-3.7.2 - System maintenance control
67	MA.L2-3.7.3 - Equipment sanitization
68	MA.L2-3.7.4 - Media inspection
69	MA.L2-3.7.5 - Nonlocal maintenance
70	MA.L2-3.7.6 - Maintenance personnel
71	MP.L2-3.8.1 - Media protection
72	MP.L2-3.8.2 - Media access
73	MP.L2-3.8.3 - Media disposal [CUI Data]
74	MP.L2-3.8.4 - Media markings
75	MP.L2-3.8.5 - Media accountability
76	MP.L2-3.8.6 - Portable storage encryption
77	MP.L2-3.8.7 - Removeable media
78	MP.L2-3.8.8 - Shared media
79	MP.L2-3.8.9 - Protect backups
80	PE.L2-3.10.1 - Limit physical access [CUI Data]
81	PE.L2-3.10.2 - Monitor facility
82	PE.L2-3.10.3 - Escort visitors [CUI Data]
83	PE.L2-3.10.4 - Physical access logs [CUI Data]
84	PE.L2-3.10.5 - Manage physical access [CUI Data]
85	PE.L2-3.10.6 - Alternative work sites
86	PS.L2-3.9.1 - Screen individuals
87	PS.L2-3.9.2 - Personnel actions
88	RA.L2-3.11.1 - Risk assessments
89	RA.L2-3.11.2 - Vulnerability scan
90	RA.L2-3.11.3 - Vulnerability remediation
91	SC.L2-3.13.1 - Boundary protection [CUI Data]
92	SC.L2-3.13.2 - Security engineering
93	SC.L2-3.13.3 - Role separation

94	SC.L2-3.13.4 - Shared resource control
95	SC.L2-3.13.5 - Public-access system separation [CUI Data]
96	SC.L2-3.13.6 - Network communication by exception
97	SC.L2-3.13.7 - Split tunneling
98	SC.L2-3.13.8 - Data in transit
99	SC.L2-3.13.9 - Connections termination
100	SC.L2-3.13.10 - Key management
101	SC.L2-3.13.11 - Cui encryption
102	SC.L2-3.13.12 - Collaborative device control
103	SC.L2-3.13.13 - Mobile code
104	SC.L2-3.13.14 - Voice over internet protocol
105	SC.L2-3.13.15 - Communications authenticity
106	SC.L2-3.13.16 - Data at rest
107	SI.L2-3.14.1 - Flaw remediation [CUI Data]
108	SI.L2-3.14.2 - Malicious code protection [CUI Data]
109	SI.L2-3.14.3 - Security alerts & advisories
110	SI.L2-3.14.4 - Update malicious code protection [CUI Data]
111	SI.L2-3.14.5 - System & file scanning [CUI Data]
112	SI.L2-3.14.6 - Monitor communications for attacks
113	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).

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.

AC.L2-3.1.1 - Authorized access control [CUI Data]

CMMC 2.13 - Level 2	Other Requirements
AC.L2-3.1.1 Authorized access control [CUI Data]	N/A

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

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

Guidance
DISCUSSION [NIST SP 800-171 REV. 2]
Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. 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. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses [sic] non-privileged) are addressed in requirement 3.1.2 (AC.L2-3.1.2).

FURTHER DISCUSSION
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.

This requirement, AC.L2-3.1.1, controls system access based on user, process, or device identity. AC.L2-3.1.1 leverages IA.L2-3.5.1 which provides a vetted and trusted identity for access control.

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

Related Internal Controls
- 3.1.1[a] - Identify - Authorized Users: Determine if authorized users are identified.
- 3.1.1[b] - Identify - Authorized Processes: Determine if processes acting on behalf of authorized users are identified.

- 3.1.1[c] - Identify - Authorized Devices: Determine if devices (and other systems) authorized to connect to the system are identified.

- 3.1.1[d] - Block - Unauthorized Users: Determine if system access is limited to authorized users.

- 3.1.1[e] - Block - Unauthorized Processes: Determine if system access is limited to processes acting on behalf of authorized users.

- 3.1.1[f] - Block - Unauthorized Devices: Determine if system access is limited to authorized devices (including other systems).

References

- DoD CIO - CMMC Documentation - https://dodcio.defense.gov/CMMC/Documentation/
- CMMC Assessment Guide Level 2 - Version 2.13 - https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_20211016_508.pdf

AC.L2-3.1.2 - Transaction & function control

CMMC 2.13 - Level 2	Other Requirements
AC.L2-3.1.2 Transaction & function control	N/A

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

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

Guidance
DISCUSSION [NIST SP 800-171 REV. 2]
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).

FURTHER DISCUSSION
Limit users to only the information systems, roles, or applications they are permitted to use and are needed for their roles and responsibilities. Limit access to applications and data based on the authorized users' roles and responsibilities. Common types of functions a user can be assigned are create, read, update, and delete.

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

Related Internal Controls
- 3.1.2[a] - Identify - Authorized Functions: Determine if the types of transactions and functions that authorized users are permitted to execute are defined.

- 3.1.2[b] - Block - Unauthorized Functions: Determine if system access is limited to the defined types of transactions and functions for authorized users.

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

AC.L2-3.1.3 - Control CUI flow

CMMC 2.13 - Level 2	Other Requirements
AC.L2-3.1.3 Control CUI flow	N/A

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

Control the flow of CUI in accordance with approved authorizations.

Guidance
DISCUSSION [NIST SP 800-171 REV. 2]
Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following:
1. keeping export-controlled information from being transmitted in the clear to the internet;
2. blocking outside traffic that claims to be from within the organization;
3. restricting requests to the internet that are not from the internal web proxy server; and
4. limiting information transfers between organizations based on data structures and content.

FURTHER DISCUSSION
Typically, companies will have a firewall between the internal network and the internet. Often multiple firewalls or routing switches are used inside a network to create zones to separate sensitive data, business units, or user groups. Proxy servers can be used to break the connection between multiple networks. All traffic entering or leaving a network is intercepted by the proxy, preventing direct access between networks. Companies should also ensure by policy and enforcement mechanisms that all CUI allowed to flow across the internet is encrypted.

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

Related Internal Controls
- 3.1.3[a] - Policy - Information Flow Control: Determine if information flow control policies are defined.
- 3.1.3[b] - Identify - CUI Flow Control: Determine if methods and enforcement mechanisms for controlling the flow of CUI are defined.
- 3.1.3[c] - Identify - CUI Boundaries: Determine if designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.
- 3.1.3[d] - Identify - CUI Authorizations: Determine if authorizations for controlling the flow of CUI are defined.

- 3.1.3[e] - Confirm - CUI Authorizations: Determine if approved authorizations for controlling the flow of CUI are enforced.

References

- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- DoD CIO - CMMC Documentation - https://dodcio.defense.gov/CMMC/Documentation/

AC.L2-3.1.4 - Separation of duties

CMMC 2.13 - Level 2	Other Requirements
AC.L2-3.1.4 Separation of duties	N/A

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

Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Guidance
DISCUSSION [NIST SP 800-171 REV. 2]
Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., configuration management, quality assurance and testing, system management, programming, and network security); and ensuring that security personnel administering access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of organizational systems and system components when developing policy on separation of duties.

FURTHER DISCUSSION
No one person should be in charge of an entire critical task from beginning to end. Documenting and dividing elements of important duties and tasks between employees reduces intentional or unintentional execution of malicious activities.

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

Related Internal Controls
- 3.1.4[a] - Identify - Separation of Duties: Determine if the duties of individuals requiring separation are defined.
- 3.1.4[b] - Confirm - Separation of Duties: Determine if responsibilities for duties that require separation are assigned to separate individuals.
- 3.1.4[c] - Confirm - Separation of Access: Determine if access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.

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

AC.L2-3.1.5 - Least privilege

CMMC 2.13 - Level 2	Other Requirements
AC.L2-3.1.5 Least privilege	N/A

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

Employ the principle of least privilege, including for specific security functions and privileged accounts.

Guidance
DISCUSSION [NIST SP 800-171 REV. 2]
Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges).

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information or functions. Organizations may differentiate in the application of this requirement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

FURTHER DISCUSSION
The principle of least privilege applies to all users and processes on all systems, but it is critical to systems containing or accessing CUI. Least privilege:

1. restricts user access to only the machines and information needed to fulfill job responsibilities; and

2. limits what system configuration settings users can change, only allowing individuals with a business need to change them.

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

Related Internal Controls
- 3.1.5[a] - Identify - Privileged Accounts: Determine if privileged accounts are identified.
- 3.1.5[b] - Confirm - Least Privilege (Privileged Accounts): Determine if access to privileged accounts is authorized in accordance with the principle of least privilege.

- 3.1.5[c] - Identify - Security Functions: Determine if security functions are identified.

- 3.1.5[d] - Confirm - Least Privilege (Functions): Determine if access to security functions is authorized in accordance with the principle of least privilege.

References

- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- DoD CIO - CMMC Documentation - https://dodcio.defense.gov/CMMC/Documentation/

AC.L2-3.1.6 - Non-privileged account use

CMMC 2.13 - Level 2	Other Requirements
AC.L2-3.1.6 Non-privileged account use	N/A

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

Use non-privileged accounts or roles when accessing nonsecurity functions.

Guidance
DISCUSSION [NIST SP 800-171 REV. 2]
This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non- privileged account.

FURTHER DISCUSSION
A user with a privileged account can perform more tasks and access more information than a person with a non-privileged account. Tasks (including unauthorized tasks orchestrated by attackers) performed when using the privileged account can have a greater impact on the system. System administrators and users with privileged accounts must be trained not to use their privileged accounts for everyday tasks, such as browsing the internet or connecting unnecessarily to other systems or services.

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

Related Internal Controls
- 3.1.6[a] - Identify - Non Security Functions: Determine if nonsecurity functions are identified.
- 3.1.6[b] - Confirm - Non Security Functions: Determine if users are required to use non-privileged accounts or roles when accessing nonsecurity functions.

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

AC.L2-3.1.7 - Privileged functions

CMMC 2.13 - Level 2	Other Requirements
AC.L2-3.1.7 Privileged functions	N/A

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

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

Guidance
DISCUSSION [NIST SP 800-171 REV. 2]
Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in 3.1.2 (AC.L2-3.1.2).

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

FURTHER DISCUSSION
Non-privileged users should receive only those permissions required to perform their basic job functions. Privileged users are granted additional permissions because their jobs require them. Privileged functions typically involve the control, monitoring, or administration of the system and its security measures. When these special privileged functions are performed, the activity must be captured in an audit log, which can be used to identify abuse. Non-privileged employees must not be granted permission to perform any of the functions of a privileged user.

This requirement, AC.L2-3.1.7, manages non-privileged users by logging any attempts to execute privileged functions. AC.L2-3.1.7 leverages AU.L2-3.3.2, which ensures logging and traceability of user actions. AC.L2-3.1.7 also extends AC.L2-3.1.2, which defines a requirement to limit types of transactions and functions to those that authorized users are permitted to execute.

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

Related Internal Controls
- 3.1.7[a] - Identify - Privileged Functions: Determine if privileged functions are defined.
- 3.1.7[b] - Identify - Non Privileged Users: Determine if non-privileged users are defined.

- 3.1.7[c] - Confirm - Non Privileged Users: Determine if non-privileged users are prevented from executing privileged functions.

- 3.1.7[d] - Confirm - Privileged Functions: Determine if the execution of privileged functions is captured in audit logs.

References

- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- DoD CIO - CMMC Documentation - https://dodcio.defense.gov/CMMC/Documentation/

AC.L2-3.1.8 - Unsuccessful logon attempts

CMMC 2.13 - Level 2	Other Requirements
AC.L2-3.1.8 Unsuccessful logon attempts	N/A

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

Limit unsuccessful logon attempts.

Guidance
DISCUSSION [NIST SP 800-171 REV. 2]
This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.

FURTHER DISCUSSION
Consecutive unsuccessful logon attempts may indicate malicious activity. OSAs can mitigate these attacks by limiting the number of unsuccessful logon attempts, typically by locking the account. A defined number of consecutive unsuccessful logon attempts is a common configuration setting. OSAs are expected to set this number at a level that fits their risk profile with the knowledge that fewer unsuccessful attempts provide higher security.

After an unsuccessful login attempt threshold is exceeded and the system locks an account, the account may either:

1. remain locked until an administrator takes action to unlock it, or
2. be locked for a predefined time after which it unlocks automatically.

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

Related Internal Controls
- 3.1.8[a] - Identify - Password Lockout: Determine if the means of limiting unsuccessful logon attempts is defined.

- 3.1.8[b] - Confirm - Password Lockout: Determine if the defined means of limiting unsuccessful logon attempts is implemented.

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

- DoD CIO - CMMC Documentation - https://dodcio.defense.gov/CMMC/Documentation/

AC.L2-3.1.9 - Privacy & security notices

CMMC 2.13 - Level 2	Other Requirements
AC.L2-3.1.9 Privacy & security notices	N/A

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

Provide privacy and security notices consistent with applicable CUI rules.

Guidance
DISCUSSION [NIST SP 800-171 REV. 2]
System use notifications can be implemented using messages or warning banners displayed before individuals log in to organizational systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Based on a risk assessment, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations consult with the Office of General Counsel for legal review and approval of warning banner content.

FURTHER DISCUSSION
Every system containing or providing access to CUI has legal requirements concerning user privacy and security notices. One method of addressing this requirement is the use of a system-use notification banner that displays the legal requirements of using the system. Users may be required to click to agree to the displayed requirements of using the system each time they log on to the machine. This agreement can be used in the civil and/or criminal prosecution of an attacker that violates the terms.

The legal notification should meet all applicable requirements. At a minimum, the notice should inform the user that:

1. information system usage may be monitored or recorded, and is subject to audit;
2. unauthorized use of the information systems is prohibited;
3. unauthorized use is subject to criminal and civil penalties;
4. use of the information system affirms consent to monitoring and recording;
5. the information system contains CUI with specific requirements imposed by the Department of Defense; and
6. use of the information system may be subject to other specified requirements associated with certain types of CUI such as Export Controlled information.

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

Related Internal Controls

- 3.1.9[a] - Identify - Security Notices: Determine if privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category.

- 3.1.9[b] - Confirm - Security Notices: Determine if privacy and security notices are displayed.

References

- Department of Defense CMMC website - https://dodcio.defense.gov/CMMC/index.html
- DoD CIO - CMMC Documentation - https://dodcio.defense.gov/CMMC/Documentation/

AC.L2-3.1.10 - Session lock

CMMC 2.13 - 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
DISCUSSION [NIST SP 800-171 REV. 2]
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.

FURTHER DISCUSSION
Session locks can be initiated by the user or, more fundamentally, enabled automatically when the system has been idle for a period of time, for example, five minutes. Session locks are a quick way to prevent unauthorized use of the systems without having a user log off. Minimum configuration requirements are left up to the organization to define.

A locked session shows pattern-hiding information on the screen to mask the data on the display.

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

Related Internal Controls
- 3.1.10[a] - Identify - Session Lock: Determine if the period of inactivity after which the system initiates a session lock is defined.
- 3.1.10[b] - Confirm - Session Lock: Determine if access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity.
- 3.1.10[c] - Confirm - Session Lock (Pattern): Determine if previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.

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

- DoD CIO - CMMC Documentation - https://dodcio.defense.gov/CMMC/Documentation/

TRUNCATED SAMPLE DOCUMENT