YourIT!
Your Logo Goes Here

CMMC Assessment

NIST 800 171 Scoring Supplement

Prepared for:
Client Company
Prepared by:
YourIT Company

Table of Contents

4.1 - Access Restrictions for Changes - CMMC Ctrl: CM.3.067 - Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.4.5)

4.2 - Least Functionality - Prevent program execution - CMMC Ctrl: CM.3.068 - Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. (NIST 800-171 Rev. 2 Ctrl Ref: 3.4.7)

4.3 - Application Blacklisting/Whitelisting - CMMC Ctrl: CM.3.069 - Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. (NIST 800-171 Rev. 2 Ctrl Ref: 3.4.8)

5 - IDENTIFICATION AND AUTHENTICATION (IA)

5.1 - Authentication - CMMC Ctrl: IA.3.083 - Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.3)

5.2 - Replay Resistent Mechanisms - CMMC Ctrl: IA.3.084 - Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.4)

5.3 - Identify Management - CMMC Ctrl: IA.3.085 - Prevent the reuse of identifiers for a defined period. (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.5)

5.4 - Identify Management - CMMC Ctrl: IA.3.086 - Disable identifiers after a defined period of inactivity. (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.6)

6 - INCIDENT RESPONSE (IR)

6.1 - Incident Reporting - CMMC Ctrl: IR.3.098 - Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. (NIST 800-171 Rev. 2 Ctrl Ref: 3.6.2)

6.2 - Incident Response Testing - CMMC Ctrl: IR.3.099 - Test the organizational incident response capability. (NIST 800-171 Rev. 2 Ctrl Ref: 3.6.3)

7 - MAINTENANCE (MA)

7.1 - Sanitize Media Before Removal Off-Site - CMMC Ctrl: MA.3.115 - Ensure equipment removed for off-site maintenance is sanitized of any CUI. (NIST 800-171 Rev. 2 Ctrl Ref: 3.7.3)

7.2 - Maintenance Tools - Inspect Media - CMMC Ctrl: MA.3.116 - Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.7.4)

8 - MEDIA PROTECTION (MP)

8.1 - Protect and Control - CMMC Ctrl: MP.3.122 - Mark media with necessary CUI markings and distribution limitations. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.4)

8.2 - Protect and Control - CMMC Ctrl: MP.3.123 - Prohibit the use of portable storage devices when such devices have no identifiable owner. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.8)

8.3 - Transported Media Access Control - CMMC Ctrl: MP.3.124 - Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.5)

8.4 - Encrypt Media During Transport - CMMC Ctrl: MP.3.125 - Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.6)

9 - PHYSICAL PROTECTION (PE)

9.1 - Alternative Site Safeguards - CMMC Ctrl: PE.3.136 - Enforce safeguarding measures for CUI at alternate work sites. (NIST 800-171 Rev. 2 Ctrl Ref: 3.10.6)

10 - SECURITY ASSESSMENT (CA)

10.1 - Continuous Monitoring - CMMC Ctrl: CA.3.161 - Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. (NIST 800-171 Rev. 2 Ctrl Ref: 3.12.3)

11 - SYSTEM AND COMMUNICATIONS PROTECTION (SC)

11.1 - Cyptographic Protection of CUI - CMMC Ctrl: SC.3.177 - Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.11)

11.2 - Security Engineering Principles - CMMC Ctrl: SC.3.180 - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.2)

11.3 - Application Partioning - CMMC Ctrl: SC.3.181 - Separate user functionality from system management functionality. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.3)

11.4 - Shared Resource Security - CMMC Ctrl: SC.3.182 - Prevent unauthorized and unintended information transfer via shared system resources. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.4)

11.5 - Deny by Default / Allow by Exception - CMMC Ctrl: SC.3.183 - Deny network communications traffic by default and allow network communications traffic by exception(i.e., deny all, permit by exception). (NIST 800 - 171 Rev. 2 Ctrl Ref: 3.13.6)

11.6 - Split Tunneling Prevention for Remote Devices - CMMC Ctrl: SC.3.184 - Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.7)

11.7 - Transmission Confidentiality and Integrity - CMMC Ctrl: SC.3.185 - Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.8)

11.8 - Connection Termination - CMMC Ctrl: SC.3.186 - Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.9)

11.9 - Cryptographic Key Establishment and Management - CMMC Ctrl: SC.3.187 - Establish and manage cryptographic keys for cryptography employed in organizational systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.10)

11.10 - Mobile Code - CMMC Ctrl: SC.3.188 - Control and monitor the use of mobile code. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.13)

11.11 - VoIP - CMMC Ctrl: SC.3.189 - Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.14)

11.12 - Session Authenticity - CMMC Ctrl: SC.3.190 - Protect the authenticity of communications sessions. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.15)

11.13 - Protection of CUI at Rest - CMMC Ctrl: SC.3.191 - Protect the confidentiality of CUI at rest. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.16)

1 - ACCESS CONTROL (AC)

1.1 - Wireless Access and Encryption - CMMC Ctrl: AC.3.012 - Protect wireless access using authentication and encryption. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.17)

Does the company protect wireless access using authentication and encryption.

Yes

Follow-up to 1.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

Organizational restrictions may vary for the different types of devices. Usage restrictions and implementation guidance for mobile devices include: device identification and authentication; configuration management; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared).

1.2 - Protect Remote Access - CMMC Ctrl: AC.3.014 - Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.13)

Do all methods used to access the system via remote access sessions use approved encryption methods?

Yes

Follow-up to 1.2 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. See the following NIST documents for mechanisms implemented [NIST CRYPTO]; [NIST CAVP]; [NIST CMVP]; National Security Agency Cryptographic Standards.

1.3 - Separation of Duties - CMMC Ctrl: AC.3.017 - Separate the duties of individuals to reduce the risk of malevolent activity without collusion. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.4)

Does the company employ the Separation of Duties Principle?

Yes

Follow-up to 1.3 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented the process, mechanism, and controls necessary to meet this security requirement.

1.4 - Privileged Function Access - CMMC Ctrl: AC.3.018 - Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.7)

Does the company have a mechanism in place to prevent non-privileged users from executing privileged functions and capture the execution of privileged functions in audit logs?

Yes

Follow-up to 1.4 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented 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.

1.5 - User Session Termination - CMMC Ctrl: AC.3.019 - Terminate (automatically) user sessions after a defined condition. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.11)

Does the company enable the automatic termination of information system user sessions?

Yes

Follow-up to 1.5 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

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.

1.6 - Mobile Device Connections - CMMC Ctrl: AC.3.020 - Control connection of mobile devices. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.18)

Has the company implemented a mechanism to control the connection of mobile devices to the information system?

Yes

Follow-up to 1.6 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different types of devices. Usage restrictions and implementation guidance for mobile devices include: device identification and authentication; configuration management; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared).

1.7 - Remote Execution - CMMC Ctrl: AC.3.021 - Authorize remote execution of privileged commands and remote access to security-relevant information. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.15)

Does the company restrict access to remote execution of privileged commands and remote access to security information?

Yes

Follow-up to 1.7 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented controls to authorize the use of privileged commands to authorize 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.

1.8 - CUI Encryption - CMMC Ctrl: AC.3.022 - Encrypt CUI on mobile devices and mobile computing platforms. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.19)

Does the company encrypt CUI on mobile devices and mobile computing platforms?

Yes

Follow-up to 1.8 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented the necessary cryptography to encrypt CUI on mobile devices and computing platforms.

2 - AUDIT AND ACCOUNTABILITY (AU)

2.1 - Review and Update Logged Events - CMMC Ctrl: AU.3.045 - Review and update logged events. (NIST 800-171 Rev. 2 Ctrl Ref: 3.3.3)

Does the company review and update audited events annually or in the event of substantial system changes or as needed?

Yes

Follow-up to 2.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization will periodically re-evaluate which logged events will continue to be included in the list of events to be logged. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient

2.2 - Response to Audit Logging Failures - CMMC Ctrl: AU.3.046 - Alert in the event of an audit logging process failure. (NIST 800-171 Rev. 2 Ctrl Ref: 3.3.4)

Will the system alert employees with security responsibilities in the event of an audit processing failure?

Yes

Follow-up to 2.2 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented mechanisms that will detect and alert upon audit logging process failures include software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded.

2.3 - Protection of Audit Information - CMMC Ctrl: AU.3.049 - Protect audit information and audit logging tools from unauthorized access, modification, and deletion. (NIST 800-171 Rev. 2 Ctrl Ref: 3.3.8)

Does the system protect audit information and audit tools from unauthorized access, modification, and deletion?

No

2.4 - Limit Log Access - CMMC Ctrl: AU.3.050 - Limit management of audit logging functionality to a subset of privileged users. (NIST 800-171 Rev. 2 Ctrl Ref: 3.3.9)

Is access to management of audit functionality authorized only to a limited subset of privileged users?

Planned

Follow-up to 2.4 if you answered Planned above
- Describe the plan to implement the controls necessary to meet this requirement.

The organization will implement practices to specify that privileged access be further defined between audit-related privileges and other privileges and authorized access granted as necessary, thus limiting the users with audit-related privileges.

2.5 - Correlate Audit Record Repositories - CMMC Ctrl: AU.3.051 - Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. (NIST 800-171 Rev. 2 Ctrl Ref: 3.3.5)

Does the company use mechanisms across different repositories to integrate audit review, analysis, correlation, and reporting processes?

Yes

Follow-up to 2.5 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization correlates audit record review, analysis, and reporting processes helps to ensure that they do not operate independently, but rather collectively throughout the organization.

2.6 - Audit Record Reduction and Report Generation - CMMC Ctrl: AU.3.052 - Provide audit record reduction and report generation to support on-demand analysis and reporting. (NIST 800-171 Rev. 2 Ctrl Ref: 3.3.6)

Does the system provide an audit reduction and report generation capability to support on-demand analysis and reporting?

Yes

Follow-up to 2.6 if you answered Yes above

- Describe the mechanism implemented to meet this control requirement.

The organization has implemented the process, mechanism, and controls necessary to meet this security requirement.

3 - AWARENESS AND TRAINING (AT)

3.1 - Insider Threat Awareness Training - CMMC Ctrl: AT.3.058 - Provide security awareness training on recognizing and reporting potential indicators of insider threat. (NIST 800-171 Rev. 2 Ctrl Ref: 3.2.3)

Does the company ensure that users, managers, and system administrators receive annual training on potential indicators and possible precursors of insider threats and other serious violations of company policies consistent with this control requirement?

Yes

Follow-up to 3.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization's security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

4 - CONFIGURATION MANAGEMENT (CM)

4.1 - Access Restrictions for Changes - CMMC Ctrl: CM.3.067 - Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.4.5)

Does the company define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems?

No

4.2 - Least Functionality - Prevent program execution - CMMC Ctrl: CM.3.068 - Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. (NIST 800-171 Rev. 2 Ctrl Ref: 3.4.7)

Does the company restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services?

Yes

Follow-up to 4.2 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has made a security-based determination which functions, ports, protocols, and/or services are restricted. Bluetooth, File Transfer Protocol (FTP), and peer-to-peer networking are examples of protocols organizations when consider the preventing the use of, restricting, or disabling.

4.3 - Application Blacklisting/Whitelisting - CMMC Ctrl: CM.3.069 - Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. (NIST 800-171 Rev. 2 Ctrl Ref: 3.4.8)

Does the company employ application deny-by-exception and deny-all, permit-by-exception policies to allow the execution of authorized software?

Yes

Follow-up to 4.3 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented the necessary processes, mechanisms, and controls to implemented Blacklisting/Whitelisting.

5 - IDENTIFICATION AND AUTHENTICATION (IA)

5.1 - Authentication - CMMC Ctrl: IA.3.083 - Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.3)

Does the company use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts?

Yes

Follow-up to 5.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, when necessary, to provide increased information security.

Follow-up to 5.1 if you answered Yes above
- Which users are required to use MFA?

Remote and privileged users only

5.2 - Replay Resistent Mechanisms - CMMC Ctrl: IA.3.084 - Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.4)

Does the company employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts?

Yes

Follow-up to 5.2 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.

5.3 - Identify Management - CMMC Ctrl: IA.3.085 - Prevent the reuse of identifiers for a defined period. (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.5)

Does the company prevent the reuse of identifiers for a defined period?

Yes

Follow-up to 5.3 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

Identifiers are provided for users, processes acting on behalf of users, or devices (3.5.1). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

5.4 - Identify Management - CMMC Ctrl: IA.3.086 - Disable identifiers after a defined period of inactivity. (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.6)

Does the company disable identifiers after a defined period of inactivity.

Yes

Follow-up to 5.4 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

Inactive identifiers pose a risk to organizational information because attackers may exploit an inactive identifier to gain undetected access to organizational devices. The owners of the inactive accounts may not notice if unauthorized access to the account has been obtained. The organization regularly performs tests to identify inactive identifiers and disables the identifiers.

6 - INCIDENT RESPONSE (IR)

6.1 - Incident Reporting - CMMC Ctrl: IR.3.098 - Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. (NIST 800-171 Rev. 2 Ctrl Ref: 3.6.2)

Does the company Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization?

Yes

Follow-up to 6.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

> The organization has implemented a practice of reporting suspected security incidents that may include the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies.

6.2 - Incident Response Testing - CMMC Ctrl: IR.3.099 - Test the organizational incident response capability. (NIST 800-171 Rev. 2 Ctrl Ref: 3.6.3)

Does the company periodically test organizational incident response capability?

> Yes

Follow-up to 6.2 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

> The organization has implemented the process, mechanism, and controls necessary to meet this security requirement.

7 - MAINTENANCE (MA)

7.1 - Sanitize Media Before Removal Off-Site - CMMC Ctrl: MA.3.115 - Ensure equipment removed for off-site maintenance is sanitized of any CUI. (NIST 800-171 Rev. 2 Ctrl Ref: 3.7.3)

Does the company ensure that all equipment remove for off-site maintenance is santized of any CUI?

> Yes

Follow-up to 7.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

> The organization has implemented practices that define information security aspects of system maintenance that are performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in- house, software maintenance agreement). In addition the organization utilizes the sanitization practices specified in [SP 800-88] that provides guidance on media sanitization

7.2 - Maintenance Tools - Inspect Media - CMMC Ctrl: MA.3.116 - Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.7.4)

Are media that are provided by authorized maintenance personnel (and not normal systems administrators/owners) for troubleshooting, diagnostics, or other maintenance run through an anti-virus/anti-malware/anti-spyware program prior to use in the company's information system?

> Yes

Follow-up to 7.2 if you answered Yes above

- Describe the mechanism implemented to meet this control requirement.

The organization has implemented the process, mechanism, and controls necessary to meet this security requirement.

8 - MEDIA PROTECTION (MP)

8.1 - Protect and Control - CMMC Ctrl: MP.3.122 - Mark media with necessary CUI markings and distribution limitations. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.4)

Does the company mark media containing CUI with the necessary CUI markings and distribution limitations?

Planned

Follow-up to 8.1 if you answered Planned above
- Describe the plan to implement the controls necessary to meet this requirement.

The organization plans to implement practices that where the use of human-readable security attributes. System media includes digital and non-digital media. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations. The organization will rely on the requirements set forth in the publication [NARA MARK].

8.2 - Protect and Control - CMMC Ctrl: MP.3.123 - Prohibit the use of portable storage devices when such devices have no identifiable owner. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.8)

Does the company prohibit use of portable storage devices that have no identifiable owner?

Yes

Follow-up to 8.2 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has a practices whereby all information system users are to request portable storage device authorization prior to use in organization information systems. After the device undergoes a physical and digital inspection, the device will be authorized for use.

8.3 - Transported Media Access Control - CMMC Ctrl: MP.3.124 - Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.5)

Does the company control access to media containing CUI and track media taken outside of controlled areas?

No

8.4 - Encrypt Media During Transport - CMMC Ctrl: MP.3.125 - Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.6)

Has the company implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards?

Yes

Follow-up to 8.4 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented mechanisms and practices to meet this requirement as it applies to portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives). . The organization relies on the guidance contained in publications [NIST CRYPTO] and [SP 800-111] which provide guidance on storage encryption technologies for end user devices.

9 - PHYSICAL PROTECTION (PE)

9.1 - Alternative Site Safeguards - CMMC Ctrl: PE.3.136 - Enforce safeguarding measures for CUI at alternate work sites. (NIST 800-171 Rev. 2 Ctrl Ref: 3.10.6)

Does the company enforce safeguarding measures for CUI at all company work sites?

No

10 - SECURITY ASSESSMENT (CA)

10.1 - Continuous Monitoring - CMMC Ctrl: CA.3.161 - Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. (NIST 800-171 Rev. 2 Ctrl Ref: 3.12.3)

Are continuous monitoring tools deployed for front internet facing systems (computers with IP addresses that can be reached from the internet) or those used to store or transmit sensitive data?

Yes

Follow-up to 10.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization performs periodic security and risk assessments in an effort to monitor control implementation and periodically maintain organization information systems to address identified vulnerabilities.

11 - SYSTEM AND COMMUNICATIONS PROTECTION (SC)

11.1 - Cyptographic Protection of CUI - CMMC Ctrl: SC.3.177 - Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.11)

Does the company employ FIPS-validated cryptography when used to protect the confidentiality of CUI?

Yes

Follow-up to 11.1 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented cryptography that supports random number generation and hash generation. Implemented cryptographic standards used include FIPS-validated cryptography and/or NSA-approved cryptography as referenced in the following NIST publications. See [NIST CRYPTO]; [NIST CAVP]; and [NIST CMVP].

Follow-up to 11.1 if you answered Yes above
- Describe the implemented cryptography used to protect CUI.

Fully FIPS validated

11.2 - Security Engineering Principles - CMMC Ctrl: SC.3.180 - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.2)

Does the company employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems?

Yes

Follow-up to 11.2 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented the process, mechanism, and controls necessary to meet this security requirement.

11.3 - Application Partioning - CMMC Ctrl: SC.3.181 - Separate user functionality from system management functionality. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.3)

Does the company employ mechanisms to separate user functionality from system management functionality?

Yes

Follow-up to 11.3 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented the process, mechanism, and controls necessary to meet this security requirement.

11.4 - Shared Resource Security - CMMC Ctrl: SC.3.182 - Prevent unauthorized and unintended information transfer via shared system resources. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.4)

Does the company employ mechanisms to prevent unauthorized and unintended information transfer via shared resources?

Yes

Follow-up to 11.4 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented mechanisms to control of information in shared system resources (e.g., registers, cache memory, main memory, hard disks) is also commonly referred to as object reuse and residual information protection. These controls prevent information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. The mechanisms have also been applied to encrypted representations of information.

11.5 - Deny by Default / Allow by Exception - CMMC Ctrl: SC.3.183 - Deny network communications traffic by default and allow network communications traffic by exception(i.e., deny all, permit by exception). (NIST 800 - 171 Rev. 2 Ctrl Ref: 3.13.6)

Does the company have a policy to configure the information system to deny network communications traffic by default and allow network traffic by exception?

Yes

Follow-up to 11.5 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The mechanism implemented by the organization limits/controls to inbound and outbound network communications traffic at the system boundary and at identified points within the system. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

11.6 - Split Tunneling Prevention for Remote Devices - CMMC Ctrl: SC.3.184 - Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.7)

Does the company employ safeguards to prevent remote devices from establishing non-remote connections to the system and communicating via some other connection to external networks?

Yes

Follow-up to 11.6 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented a mechanisms to control remote devices (e.g., notebook computers, smart phones, and tablets) through configuration settings to disable split tunneling in those devices, and by preventing configuration settings from being readily configurable by users. Mechanisms are implemented in the system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.

11.7 - Transmission Confidentiality and Integrity - CMMC Ctrl: SC.3.185 - Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.8)

Has the company implemented cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards?

Yes

Follow-up to 11.7 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented a physical safeguard in the form of a protected distribution system (PDS) where the distribution medium is protected against electronic or physical intercept, thereby ensuring the confidentiality of the information being transmitted.

11.8 - Connection Termination - CMMC Ctrl: SC.3.186 - Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.9)

Does the system terminate a network connection at the end of a session or after a defined timeframe of inactivity?

Yes

Follow-up to 11.8 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented mechanisms to terminate network connections associated with communications sessions include de-allocating associated TCP/IP address or port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. The organization has established time periods of user inactivity which includes time periods by type of network access or for specific network accesses.

11.9 - Cryptographic Key Establishment and Management - CMMC Ctrl: SC.3.187 - Establish and manage cryptographic keys for cryptography employed in organizational systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.10)

Has the company implemented procedures to establish and manage cryptography employed in organizational systems?

No

11.10 - Mobile Code - CMMC Ctrl: SC.3.188 - Control and monitor the use of mobile code. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.13)

Does the company control and monitor the use of mobile code?

Yes

Follow-up to 11.10 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

Our organization has implemented the necessary processes, mechanisms, and controls to meet the requirements for this control requirement.

11.11 - VoIP - CMMC Ctrl: SC.3.189 - Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.14)

Does the company employ the use of VoIP on organizational information systems?

Yes

Follow-up to 11.11 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

Our organization has implemented the necessary processes, mechanisms, and controls to meet the requirements for this control requirement.

11.12 - Session Authenticity - CMMC Ctrl: SC.3.190 - Protect the authenticity of communications sessions. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.15)

Has the company implemented a mechanism to protect the authenticy of communications sessions?

Yes

Follow-up to 11.12 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented the process, mechanism, and controls necessary to meet this security requirement.

11.13 - Protection of CUI at Rest - CMMC Ctrl: SC.3.191 - Protect the confidentiality of CUI at rest. (NIST 800-171 Rev. 2 Ctrl Ref: 3.13.16)

Are there controls used to protect CUI while stored in company information systems at rest?

Yes

Follow-up to 11.13 if you answered Yes above
- Describe the mechanism implemented to meet this control requirement.

The organization has implemented the use of cryptographic mechanisms and file share scanning. The organization uses other controls including secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest. The organization has implemented the related practices as described in the publication [NIST CRYPTO].