July 22nd 2024

Last change: [Date]

**CMMC Level 1 System Security Plan**

**Contents**

[**Record of Changes** 2](#_Toc160611368)

[**Scoped Contractor System Identification** 3](#_Toc160611369)

[**Scoped Contractor System Environment** 5](#_Toc160611370)

[**Domain 1: Access Control (AC)** 6](#_Toc160611371)

[**Domain 5: Identification and Authentication (IA)** 10](#_Toc160611372)

[**Domain 8: Media Protection (MP)** 12](#_Toc160611373)

[**Domain 10: Physical Protection (PE)** 13](#_Toc160611374)

[**Domain 13: System and Communications Protection (SC)** 17](#_Toc160611375)

[**Domain 14: System and Information Integrity (SI)** 20](#_Toc160611376)

# **Record of Changes**

|  |  |  |
| --- | --- | --- |
| **Date** | **Description** | **Updated By** |
|  |  |  |
| Jan 1, 2024 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# **Scoped Contractor System Identification**

**Scoped Contractor System Name/Title:** [*State the name of the system. Spell out acronyms*]

**Scoped Contractor System Categorization:**

**Scoped Contractor System Unique Identifier:** [*Insert the System Unique Identifier*]

**CMMC Contractor**

|  |  |
| --- | --- |
| Name |  |
| Address |  |
| Phone Number |  |

**Information Owner** (Government point of contact responsible for providing and/or receiving CUI)

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Office Address |  |
| Work Phone |  |
| Email Address |  |

**Scoped Contractor System Owner** (Assignment of security responsibilities)

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Office Address |  |
| Work Phone |  |
| Email Address |  |

**Contractor System Security Officer**

|  |  |
| --- | --- |
| Name |  |
| Title |   |
| Office Address |  |
| Work Phone |  |
| Email Address |  |

**General Description/Purpose of System:** What is the function/purpose of the system?

[Proved a short, high-level description of the function/purpose of the system.]

**Number of end users and privileged users:** [Provide the *approximate* number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, local administrators, etc. Add rows to define the different roles as needed.]

**Roles of Users and Number of Each Type:**

|  |  |
| --- | --- |
| Number of Users | Number of Administrators/Privileged Users |
| 0 | 0 |

**General Description of Information:** CUI information types processed, stored, or transmitted by the system are determined and documented. [Document the CUI information types processed, stored, or transmitted by the system below.]

# **Scoped Contractor System Environment**

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note: this does not require depicting every workstation or desktop, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.

[Insert a network diagram. Provide a narrative consistent with the diagram that clearly lists and describes each system component]

* Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component. [Insert the reference URL or note that the hardware component inventory is attached.]
* List all software components installed on the Scoped Contractor CMMC system. [Insert the reference URL or note that the software component inventory is attached.]
* Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization? [Yes/No – If No, explain]

# **Domain 1: Access Control (AC)**

|  |  |
| --- | --- |
| **AC.L1-3.1.1**Authorized Access Control | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status**  |
| **[a]** Authorized users are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** Processes acting on behalf of authorized users are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[c]** Devices (and other systems) authorized to connect to the system are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[d]** System access is limited to authorized users. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[e]** System access is limited to processes acting on behalf of authorized users. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[f]** System access is limited to authorized devices (including other systems) | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** Limit Information System Access Policy**Procedure Reference:** Limit Information System Access Procedure**Evidence Reference:** https://internalcompany.com/share/CMMC/policies&procedures, https://internalcompany.com/share/CMMC/evidence |

|  |  |
| --- | --- |
| **AC.L1-3.1.2**Transaction & Function Control | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** The types of transactions and functions that authorized users are permitted to execute are defined. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** System access is limited to the defined types of transactions and functions for authorized users. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** Limit System Access to Types of Transactions Policy**Procedure Reference:** Limit System Access to Types of Transactions Policy**Evidence Reference:** |

|  |  |
| --- | --- |
| **AC.L1-3.1.20**External Connections | Verify and control/limit connections to and use of external information systems. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** Connections to external systems are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** The use of external systems is identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[c]** Connections to external systems are verified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[d]** The use of external systems is verified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[e]** Connections to external systems are controlled/limited. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[f]** The use of external systems is controlled/limited. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

|  |  |
| --- | --- |
| **AC.L1-3.1.22**Control Public Information | Control information posted or processed on publicly accessible information systems. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** Individuals authorized to post or process information on publicly accessible systems are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** Procedures to ensure FCI is not posted or processed on publicly accessible systems are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[c]** A review process is in place prior to posting of any content to publicly accessible systems. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[d]** Content on publicly accessible systems is reviewed to ensure that it does not include FCI. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[e]** Mechanisms are in place to remove and address improper posting of FCI. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

# **Domain 5: Identification and Authentication (IA)**

|  |  |
| --- | --- |
| **IA.L1-3.5.1**Identification | Identify information system users, processes acting on behalf of users, or devices. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** System users are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** Processes acting on behalf of users are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[c]** Devices accessing the system are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

|  |  |
| --- | --- |
| **IA.L1-3.5.2**Identification | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** The identity of each user is authenticated or verified as a prerequisite to system access. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[c]** The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

# **Domain 8: Media Protection (MP)**

|  |  |
| --- | --- |
| **MP.L1-3.8.3**Media Disposal | Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** System media containing FCI is sanitized or destroyed before disposal. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** System media containing FCI is sanitized before it is released for reuse. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

# **Domain 10: Physical Protection (PE)**

|  |  |
| --- | --- |
| **PE.L1-3.10.1**Limit Physical Access | Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** Authorized individuals allowed physical access are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** Physical access to organizational systems is limited to authorized individuals. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[c]** Physical access to equipment is limited to authorized individuals. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[d]** Physical access to operating environments is limited to authorized individuals. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

|  |  |
| --- | --- |
| **PE.L1-3.10.3**Escort Visitors | Escort visitors and monitor visitor activity. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** Visitors are escorted. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** Visitor activity is monitored. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

|  |  |
| --- | --- |
| **PE.L1-3.10.4**Physical Access Logs | Maintain audit logs of physical access. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** Audit logs of physical access are maintained. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

|  |  |
| --- | --- |
| **PE.L1-3.10.5**Manage Physical Access | Control and manage physical access devices. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** Physical access devices are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** Physical access devices are controlled. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[c]** Physical access devices are managed. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

# **Domain 13: System and Communications Protection (SC)**

|  |  |
| --- | --- |
| **SC.L1-3.13.1**Boundary Protection | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** The external system boundary is defined. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** Key internal system boundaries are defined. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[c]** Communications are monitored at the external system boundary. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[d]** Communications are monitored at key internal boundaries. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[e]** Communications are controlled at the external system boundary. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[f]** Communications are controlled at key internal boundaries. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[g]** Communications are protected at the external system boundary. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[h]** Communications are protected at key internal boundaries. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

|  |  |
| --- | --- |
| **SC.L1-3.13.5**Public-Access System Separation | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** Publicly accessible system components are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** Subnetworks for publicly accessible system components are physically or logically separated from internal networks. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

# **Domain 14: System and Information Integrity (SI)**

|  |  |
| --- | --- |
| **SI.L1-3.14.1**Flaw Remediation | Identify, report, and correct information and information system flaws in a timely manner. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** The time within which to identify system flaws is specified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** System flaws are identified within the specified time frame. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[c]** The time within which to report system flaws is specified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[d]** System flaws are reported within the specified time frame. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[e]** The time within which to correct system flaws is specified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[f]** System flaws are corrected within the specified time frame. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

|  |  |
| --- | --- |
| **SI.L1-3.14.2**Malicious Code Protection | Provide protection from malicious code at appropriate locations within organizational information systems. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** Publicly accessible system components are identified. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** Protection from malicious code at designated locations is provided. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

|  |  |
| --- | --- |
| **SI.L1-3.14.4**Update Malicious Code Protection | Update malicious code protection mechanisms when new releases are available. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** Malicious code protection mechanisms are updated when new releases are available. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |

|  |  |
| --- | --- |
| **SI.L1-3.14.5**System & File Scanning | Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. |
| **Responsible Role:** |
| **Assessment Objective(s)** | **Implementation Status** |
| **[a]** The frequency for malicious code scans is defined. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[b]** Malicious code scans are performed with the defined frequency. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **[c]** Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed. | [ ] Met [ ] Not Met [ ] N/A |
| **Assessment objective conformity statement:** |
| **Policy Reference:** **Procedure Reference:** **Evidence Reference:** |