[INSERT COMPANY NAME]

CMMC 2.0

System Security Plan

[INSERT COMPANY LOGO]

**Table of Contents**

[**System Security Plan** 1](#_Toc157117113)

[**1. Information System Name/Title** 2](#_Toc157117114)

[**1.1. System Function or Purpose** 2](#_Toc157117115)

[**1.2. System Function or Purpose** 2](#_Toc157117116)

[**2. CMMC 2.0** 3](#_Toc157117117)

[**3. Information System Owner** 3](#_Toc157117118)

[**4. Other Designated Contacts** 3](#_Toc157117119)

[**5. Leveraged Authorizations** 4](#_Toc157117120)

[**6. General System Description** 4](#_Toc157117121)

[**6.1. System Function or Purpose** 4](#_Toc157117122)

[**6.2. Information System Components and Boundaries** 4](#_Toc157117123)

[**6.3. Network Architecture** 5](#_Toc157117124)

[**7. System Interconnections** 5](#_Toc157117125)

[**8. Practices** 5](#_Toc157117126)

# **1.** **Information System Name/Title**

This System Security Plan provides an overview of the security requirements for the Information System Name and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed, or stored by the information system.

The security safeguards implemented for the system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures, and practices.

###### Table 1-1. Information System Name and Title

| Unique Identifier | Information System Name | Information System |
| --- | --- | --- |
|  |  |  |

# **2. CMMC 2.0**

[INSERT COMPANY NAME] has reviewed security practices and put processes in place for their information systems and anticipates receiving or maintaining CMMC 2.0 from an accredited C3PAO.

# **3. Information System Owner**

The following individual is identified as the system owner or functional proponent/advocate for this system.

##### Table 3-1 Information System Owner

|  |  |
| --- | --- |
| Information System Owner Information | |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

# **4. Other Designated Contacts**

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Table 4-1 Information System Management Point of Contact

|  |  |
| --- | --- |
| Information System Management Point of Contact | |
| Name |  |
| Title |  |
| Company / Organization |  |
| Address |  |
| Phone Number |  |
| Email Address |  |

# **5. Leveraged Authorizations**

[INSERT COMPANY NAME] may utilize the practices and processes of external organizations or service providers to operate the system. External organizations or service providers, if utilized by [INSERT COMPANY NAME] are identified below.

Table 5-1 Leveraged Authorizations

| Leveraged Information System Name | Leveraged Service Provider Owner | Date Granted |
| --- | --- | --- |
|  |  |  |

# **6. General System Description**

This section includes a general description of the [INSTERT NAME OF SYSTEM]

## **6.1. System Function or Purpose**

[INSERT FUNCTION OR PURPOSE]

## **6.2. Information System Components and Boundaries**

The System Boundary Diagram seen below provides a visual depiction of the System Boundary. The boundary separating in-scope components from out-of-scope components is depicted as a noticeable border.

**[INSERT BOUNDARY DIAGRAM]**

Figure 6-2 Authorization Boundary Diagram

## **6.3. Network Architecture**

The Network Diagram seen below provides a visual depiction of the system network components that constitute the [INSERT NAME OF SYSTEM].

**[INSERT NETWORK ARCHITECTURE DIAGRAM]**

Figure 6-3 Network Diagram

## **6.4. System Environments**

###### Table 6-1. System Environments

| **Environment** | |
| --- | --- |
| Environment Name | [INSERT] |
| Environment Type | [INSERT] |
| Operational Description | [INSERT] |

# **7. System Interconnections**

# Table 7-1. System Interconnections

| SP IP Address and Interface | External Organization Name and IP Address of System | External Point of Contact and Phone Number | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.) | Data Direction (incoming, outgoing, or both) | Information Being Transmitted | Port or Circuit Numbers |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |

# **8. Practices**

|  |  |
| --- | --- |
| C001 | Access Control (AC) |
| Access Control activities ensure that access granted to organizational systems and information is commensurate with defined access requirements. Access requirements are developed based on the organization's needs balanced with the security requirements needed to protect the organization's assets. | |

|  |  |
| --- | --- |
| AC.L1-3.1.1 | Authorized Access Control (AC.L1-3.1.1) | |
| Main Control Description: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Authorized users are identified. | No Answer |
| [b] Processes acting on behalf of authorized users are identified. | No Answer |
| [c] Devices (and other systems) authorized to connect to the system are identified. | No Answer |
| [d] System access is limited to authorized users. | No Answer |
| [e] System access is limited to processes acting on behalf of authorized users. | No Answer |
| [f] System access is limited to authorized devices (including other systems). | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f] | |

|  |  |
| --- | --- |
| AC.L1-3.1.2 | Transaction & Function Control (AC.L1-3.1.2) | |
| Main Control Description: Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The types of transactions and functions that authorized users are permitted to execute are defined. | No Answer |
| [b] System access is limited to the defined types of transactions and functions for authorized users. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AC.L2-3.1.3 | Control CUI Flow (AC.L2-3.1.3) | |
| Main Control Description: Control the flow of CUI in accordance with approved authorizations. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Information flow control policies are defined. | No Answer |
| [b] Methods and enforcement mechanisms for controlling the flow of CUI are defined. | No Answer |
| [c] Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified. | No Answer |
| [d] Authorizations for controlling the flow of CUI are defined. | No Answer |
| [e] Approved authorizations for controlling the flow of CUI are enforced. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e] | |

|  |  |
| --- | --- |
| AC.L2-3.1.4 | Separation of Duties (AC.L2-3.1.4) | |
| Main Control Description: Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The duties of individuals requiring separation are defined. | No Answer |
| [b] Responsibilities for duties that require separation are assigned to separate individuals. | No Answer |
| [c] Access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| AC.L2-3.1.5 | Least Privilege (AC.L2-3.1.5) | |
| Main Control Description: Employ the principle of least privilege, including for specific security functions and privileged accounts | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Privileged accounts are identified. | No Answer |
| [b] Access to privileged accounts is authorized in accordance with the principle of least privilege. | No Answer |
| [c] Security functions are identified. | No Answer |
| [d] Access to security functions is authorized in accordance with the principle of least privilege. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| AC.L2-3.1.6 | Non-Privileged Account Use (AC.L2-3.1.6) | |
| Main Control Description: Use non-privileged accounts or roles when accessing non-security functions. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Nonsecurity functions are identified. | No Answer |
| [b] Users are required to use non-privileged accounts or roles when accessing nonsecurity functions. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AC.L2-3.1.7 | Privileged Functions (AC.L2-3.1.7) | |
| Main Control Description: Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Privileged functions are defined. | No Answer |
| [b] Non-privileged users are defined. | No Answer |
| [c] Non-privileged users are prevented from executing privileged functions. | No Answer |
| [d] The execution of privileged functions is captured in audit logs. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| AC.L2-3.1.8 | Unsuccessful Logon Attempts (AC.L2-3.1.8) | |
| Main Control Description: Limit unsuccessful logon attempts. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The means of limiting unsuccessful logon attempts is defined. | No Answer |
| [b] The defined means of limiting unsuccessful logon attempts is implemented. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AC.L2-3.1.9 | Privacy & Security Notices (AC.L2-3.1.9) | |
| Main Control Description: Provide privacy and security notices consistent with applicable CUI rules. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category. | No Answer |
| [b] Privacy and security notices are displayed. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AC.L2-3.1.10 | Session Lock (AC.L2-3.1.10) | |
| Main Control Description: Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The period of inactivity after which the system initiates a session lock is defined. | No Answer |
| [b] Access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity. | No Answer |
| [c] Previously visible information is concealed via a pattern-hiding display after the defined period of inactivity. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| AC.L2-3.1.11 | Session Termination (AC.L2-3.1.11) | |
| Main Control Description: Terminate (automatically) user sessions after a defined condition. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Conditions requiring a user session to terminate are defined. | No Answer |
| [b] A user session is automatically terminated after any of the defined conditions occur. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AC.L2-3.1.12 | Control Remote Access (AC.L2-3.1.12) | |
| Main Control Description: Monitor and control remote access sessions. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Remote access sessions are permitted. | No Answer |
| [b] The types of permitted remote access are identified. | No Answer |
| [c] Remote access sessions are controlled. | No Answer |
| [d] Remote access sessions are monitored. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| AC.L2-3.1.13 | Remote Access Confidentiality (AC.L2-3.1.13) | |
| Main Control Description: Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Cryptographic mechanisms to protect the confidentiality of remote access sessions are identified. | No Answer |
| [b] Cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AC.L2-3.1.14 | Remote Access Routing (AC.L2-3.1.14) | |
| Main Control Description: Route remote access via managed access control points. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Managed access control points are identified and implemented. | No Answer |
| [b] Remote access is routed through managed network access control points. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AC.L2-3.1.15 | Privileged Remote Access (AC.L2-3.1.15) | |
| Main Control Description: Authorize remote execution of privileged commands and remote access to security-relevant information. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Privileged commands authorized for remote execution are identified. | No Answer |
| [b] Security-relevant information authorized to be accessed remotely is identified. | No Answer |
| [c] The execution of the identified privileged commands via remote access is authorized. | No Answer |
| [d] Access to the identified security-relevant information via remote access is authorized. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| AC.L2-3.1.16 | Wireless Access Authorization (AC.L2-3.1.16) | |
| Main Control Description: Authorize wireless access prior to allowing such connections. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Wireless access points are identified. | No Answer |
| [b] Wireless access is authorized prior to allowing such connections. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AC.L2-3.1.17 | Wireless Access Protection (AC.L2-3.1.17) | |
| Main Control Description: Protect wireless access using authentication and encryption. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Wireless access to the system is protected using authentication. | No Answer |
| [b] Wireless access to the system is protected using encryption. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AC.L2-3.1.18 | Mobile Device Connection (AC.L2-3.1.18) | |
| Main Control Description: Control connection of mobile devices. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Mobile devices that process, store, or transmit CUI are identified. | No Answer |
| [b] Mobile device connections are authorized. | No Answer |
| [c] Mobile device connections are monitored and logged. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| AC.L2-3.1.19 | Encrypt CUI on Mobile (AC.L2-3.1.19) | |
| Main Control Description: Encrypt CUI on mobile devices and mobile computing platforms. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Mobile devices and mobile computing platforms that process, store, or transmit CUI are identified. | No Answer |
| [b] Encryption is employed to protect CUI on identified mobile devices and mobile computing platforms. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AC.L1-3.1.20 | External Connections (AC.L1-3.1.20) | |
| Main Control Description: Verify and control/limit connections to and use of external information systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Connections to external systems are identified. | No Answer |
| [b] The use of external systems is identified. | No Answer |
| [c] Connections to external systems are verified. | No Answer |
| [d] The use of external systems is verified. | No Answer |
| [e] Connections to external systems are controlled/limited. | No Answer |
| [f] The use of external systems is controlled/limited. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f] | |

|  |  |
| --- | --- |
| AC.L2-3.1.21 | Portable Storage Use (AC.L2-3.1.21) | |
| Main Control Description: Limit use of portable storage devices on external systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The use of portable storage devices containing CUI on external systems is identified and documented. | No Answer |
| [b] Limits on the use of portable storage devices containing CUI on external systems are defined. | No Answer |
| [c] The use of portable storage devices containing CUI on external systems is limited as defined. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| AC.L1-3.1.22 | Control Public Information (AC.L1-3.1.22) | |
| Main Control Description: Control information posted or processed on publicly accessible information systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Individuals authorized to post or process information on publicly accessible systems are identified. | No Answer |
| [b] Procedures to ensure CUI is not posted or processed on publicly accessible systems are identified. | No Answer |
| [c] A review process is in place prior to posting of any content to publicly accessible systems. | No Answer |
| [d] Content on publicly accessible systems is reviewed to ensure that it does not include CUI. | No Answer |
| [e] Mechanisms are in place to remove and address improper posting of CUI. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e] | |

|  |  |
| --- | --- |
| C002 | Awareness and Training (AT) |
| Awareness and Training activities in an organization help to ensure staff are aware of security risks associated with their activities and roles as well as provide information security-related training that is required for employees to carry out their duties and responsibilities. | |

|  |  |
| --- | --- |
| AT.L2-3.2.1 | Role-Based Risk Awareness (AT.L2-3.2.1) | |
| Main Control Description: Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Security risks associated with organizational activities involving CUI are identified. | No Answer |
| [b] Policies, standards, and procedures related to the security of the system are identified. | No Answer |
| [c] Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities. | No Answer |
| [d] Managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| AT.L2-3.2.2 | Role-Based Training (AT.L2-3.2.2) | |
| Main Control Description: Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Information security-related duties, roles, and responsibilities are defined. | No Answer |
| [b] Information security-related duties, roles, and responsibilities are assigned to designated personnel. | No Answer |
| [c] Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| AT.L2-3.2.3 | Insider Threat Awareness (AT.L2-3.2.3) | |
| Main Control Description: Provide security awareness training on recognizing and reporting potential indicators of insider threat. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Potential indicators associated with insider threats are identified. | No Answer |
| [b] Security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| C003 | Audit and Accountability (AU) |
| Audit and Accountability is defined as a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result to ensure that the actions of an entity may be traced uniquely to that entity. | |

|  |  |
| --- | --- |
| AU.L2-3.3.1 | System Auditing (AU.L2-3.3.1) | |
| Main Control Description: Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified. | No Answer |
| [b] The content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined. | No Answer |
| [c] Audit records are created (generated). | No Answer |
| [d] Audit records, once created, contain the defined content. | No Answer |
| [e] Retention requirements for audit records are defined. | No Answer |
| [f] Audit records are retained as defined. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f] | |

|  |  |
| --- | --- |
| AU.L2-3.3.2 | User Accountability (AU.L2-3.3.2) | |
| Main Control Description: Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The content of the audit records needed to support the ability to uniquely trace users to their actions is defined. | No Answer |
| [b] Audit records, once created, contain the defined content. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AU.L2-3.3.3 | Event Review (AU.L2-3.3.3) | |
| Main Control Description: Review and update logged events. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] A process for determining when to review logged events is defined. | No Answer |
| [b] Event types being logged are reviewed in accordance with the defined review process. | No Answer |
| [c] Event types being logged are updated based on the review. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| AU.L2-3.3.4 | Audit Failure Alerting (AU.L2-3.3.4) | |
| Main Control Description: Alert in the event of an audit logging process failure. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Personnel or roles to be alerted in the event of an audit logging process failure are identified. | No Answer |
| [b] Types of audit logging process failures for which alert will be generated are defined. | No Answer |
| [c] Identified personnel or roles are alerted in the event of an audit logging process failure. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| AU.L2-3.3.5 | Audit Correlation (AU.L2-3.3.5) | |
| Main Control Description: Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined. | No Answer |
| [b] Defined audit record review, analysis, and reporting processes are correlated. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AU.L2-3.3.6 | Reduction & Reporting (AU.L2-3.3.6) | |
| Main Control Description: Provide audit record reduction and report generation to support on-demand analysis and reporting. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] An audit record reduction capability that supports on-demand analysis is provided. | No Answer |
| [b] A report generation capability that supports on-demand reporting is provided. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| AU.L2-3.3.7 | Authoritative Time Source (AU.L2-3.3.7) | |
| Main Control Description: Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Internal system clocks are used to generate time stamps for audit records. | No Answer |
| [b] An authoritative source with which to compare and synchronize internal system clocks is specified. | No Answer |
| [c] Internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| AU.L2-3.3.8 | Audit Protection (AU.L2-3.3.8) | |
| Main Control Description: Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Audit information is protected from unauthorized access. | No Answer |
| [b] Audit information is protected from unauthorized modification. | No Answer |
| [c] Audit information is protected from unauthorized deletion. | No Answer |
| [d] Audit logging tools are protected from unauthorized access. | No Answer |
| [e] Audit logging tools are protected from unauthorized modification. | No Answer |
| [f] Audit logging tools are protected from unauthorized deletion. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f] | |

|  |  |
| --- | --- |
| AU.L2-3.3.9 | Audit Management (AU.L2-3.3.9) | |
| Main Control Description: Limit management of audit logging functionality to a subset of privileged users. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] A subset of privileged users granted access to manage audit logging functionality is defined. | No Answer |
| [b] Management of audit logging functionality is limited to the defined subset of privileged users. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| C004 | Configuration Management (CM) |
| Configuration Management activities focus on defining the configuration and change management processes. | |

|  |  |
| --- | --- |
| CM.L2-3.4.1 | System Baselining (CM.L2-3.4.1) | |
| Main Control Description: Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] A baseline configuration is established. | No Answer |
| [b] The baseline configuration includes hardware, software, firmware, and documentation. | No Answer |
| [c] The baseline configuration is maintained (reviewed and updated) throughout the system development life cycle. | No Answer |
| [d] A system inventory is established. | No Answer |
| [e] The system inventory includes hardware, software, firmware, and documentation. | No Answer |
| [f] The inventory is maintained (reviewed and updated) throughout the system development life cycle. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f] | |

|  |  |
| --- | --- |
| CM.L2-3.4.2 | Security Configuration Enforcement (CM.L2-3.4.2) | |
| Main Control Description: Establish and enforce security configuration settings for information technology products employed in organizational systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Security configuration settings for information technology products employed in the system are established and included in the baseline configuration. | No Answer |
| [b] Security configuration settings for information technology products employed in the system are enforced. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| CM.L2-3.4.3 | System Change Management (CM.L2-3.4.3) | |
| Main Control Description: Track, review, approve, or disapprove, and log changes to organizational systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Changes to the system are tracked. | No Answer |
| [b] Changes to the system are reviewed. | No Answer |
| [c] Changes to the system are approved or disapproved. | No Answer |
| [d] Changes to the system are logged. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| CM.L2-3.4.4 | Security Impact Analysis (CM.L2-3.4.4) | |
| Main Control Description: Analyze the security impact of changes prior to implementation. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if the security impact of changes to the system is analyzed prior to implementation. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| CM.L2-3.4.5 | Access Restrictions for Change (CM.L2-3.4.5) | |
| Main Control Description: Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Physical access restrictions associated with changes to the system are defined. | No Answer |
| [b] Physical access restrictions associated with changes to the system are documented. | No Answer |
| [c] Physical access restrictions associated with changes to the system are approved. | No Answer |
| [d] Physical access restrictions associated with changes to the system are enforced. | No Answer |
| [e] Logical access restrictions associated with changes to the system are defined. | No Answer |
| [f] Logical access restrictions associated with changes to the system are documented. | No Answer |
| [g] Logical access restrictions associated with changes to the system are approved. | No Answer |
| [h] Logical access restrictions associated with changes to the system are enforced. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f]  [g]  [h] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f]  [g]  [h] | |

|  |  |
| --- | --- |
| CM.L2-3.4.6 | Least Functionality (CM.L2-3.4.6) | |
| Main Control Description: Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Essential system capabilities are defined based on the principle of least functionality. | No Answer |
| [b] The system is configured to provide only the defined essential capabilities. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| CM.L2-3.4.7 | Nonessential Functionality (CM.L2-3.4.7) | |
| Main Control Description: Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Essential programs are defined. | No Answer |
| [b] The use of nonessential programs is defined. | No Answer |
| [c] The use of nonessential programs is restricted, disabled, or prevented as defined. | No Answer |
| [d] Essential functions are defined. | No Answer |
| [e] The use of nonessential functions is defined. | No Answer |
| [f] The use of nonessential functions is restricted, disabled, or prevented as defined. | No Answer |
| [g] Essential ports are defined. | No Answer |
| [h] The use of nonessential ports is defined. | No Answer |
| [i] The use of nonessential ports is restricted, disabled, or prevented as defined. | No Answer |
| [j] Essential protocols are defined. | No Answer |
| [k] The use of nonessential protocols is defined. | No Answer |
| [l] The use of nonessential protocols is restricted, disabled, or prevented as defined. | No Answer |
| [m] Essential services are defined. | No Answer |
| [n] The use of nonessential services is defined. | No Answer |
| [o] The use of nonessential services is restricted, disabled, or prevented as defined. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f]  [g]  [h]  [i]  [j]  [k]  [l]  [m]  [n]  [o] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f]  [g]  [h]  [i]  [j]  [k]  [l]  [m]  [n]  [o] | |

|  |  |
| --- | --- |
| CM.L2-3.4.8 | Application Execution Policy (CM.L2-3.4.8) | |
| Main Control Description: 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. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] A policy specifying whether whitelisting or blacklisting is to be implemented is specified. | No Answer |
| [b] The software allowed to execute under whitelisting or denied use under blacklisting is specified. | No Answer |
| [c] Whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| CM.L2-3.4.9 | User-Installed Software (CM.L2-3.4.9) | |
| Main Control Description: Control and monitor user-installed software. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] A policy for controlling the installation of software by users is established. | No Answer |
| [b] Installation of software by users is controlled based on the established policy. | No Answer |
| [c] Installation of software by users is monitored. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| C005 | Identification and Authentication (IA) |
| Identification and Authentication domain activities ensure identities who have access to CUI are established, managed, and authenticated in accordance with CUI protection requirements. | |

|  |  |
| --- | --- |
| IA.L1-3.5.1 | Identification (IA.L1-3.5.1) | |
| Main Control Description: Identify information system users, processes acting on behalf of users, or devices. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] System users are identified. | No Answer |
| [b] Processes acting on behalf of users are identified. | No Answer |
| [c] Devices accessing the system are identified. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| IA.L1-3.5.2 | Authentication (IA.L1-3.5.2) | |
| Main Control Description: Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The identity of each user is authenticated or verified as a prerequisite to system access. | No Answer |
| [b] The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access. | No Answer |
| [c] The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| IA.L2-3.5.3 | Multifactor Authentication (IA.L2-3.5.3) | |
| Main Control Description: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Privileged accounts are identified. | No Answer |
| [b] Multifactor authentication is implemented for local access to privileged accounts. | No Answer |
| [c] Multifactor authentication is implemented for network access to privileged accounts. | No Answer |
| [d] Multifactor authentication is implemented for network access to non-privileged accounts. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| IA.L2-3.5.4 | Replay-Resistant Authentication (IA.L2-3.5.4) | |
| Main Control Description: Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| IA.L2-3.5.5 | Identifier Reuse (IA.L2-3.5.5) | |
| Main Control Description: Prevent reuse of identifiers for a defined period. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] A period within which identifiers cannot be reused is defined. | No Answer |
| [b] Reuse of identifiers is prevented within the defined period. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| IA.L2-3.5.6 | Identifier Handling (IA.L2-3.5.6) | |
| Main Control Description: Disable identifiers after a defined period of inactivity. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] A period of inactivity after which an identifier is disabled is defined. | No Answer |
| [b] Identifiers are disabled after the defined period of inactivity. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| IA.L2-3.5.7 | Password Complexity (IA.L2-3.5.7) | |
| Main Control Description: Enforce a minimum password complexity and change of characters when new passwords are created. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Password complexity requirements are defined. | No Answer |
| [b] Password change of character requirements are defined. | No Answer |
| [c] Minimum password complexity requirements as defined are enforced when new passwords are created. | No Answer |
| [d] Minimum password change of character requirements as defined are enforced when new passwords are created. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| IA.L2-3.5.8 | Password Reuse (IA.L2-3.5.8) | |
| Main Control Description: Prohibit password reuse for a specified number of generations. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The number of generations during which a password cannot be reused is specified. | No Answer |
| [b] Reuse of passwords is prohibited during the specified number of generations. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| IA.L2-3.5.9 | Temporary Passwords (IA.L2-3.5.9) | |
| Main Control Description: Allow temporary password use for system logons with an immediate change to a permanent password. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if an immediate change to a permanent password is required when a temporary password is used for system logon. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| IA.L2-3.5.10 | Cryptographically-Protected Passwords (IA.L2-3.5.10) | |
| Main Control Description: Store and transmit only cryptographically-protected passwords. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Passwords are cryptographically protected in storage. | No Answer |
| [b] Passwords are cryptographically protected in transit. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| IA.L2-3.5.11 | Obscure Feedback (IA.L2-3.5.11) | |
| Main Control Description: Obscure feedback of authentication information. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if authentication information is obscured during the authentication process. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| C006 | Incident Response (IR) |
| A cybersecurity event is any observable occurrence that affects organizational assets and has the potential to disrupt operations. A cybersecurity incident is an event or series of events that significantly affects or could significantly affect organizational assets and services and requires the organization (and possibly other stakeholders) to respond in some way to prevent or limit adverse impacts. | |

|  |  |
| --- | --- |
| IR.L2-3.6.1 | Incident Handling (IR.L2-3.6.1) | |
| Main Control Description: Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] An operational incident-handling capability is established. | No Answer |
| [b] The operational incident-handling capability includes preparation. | No Answer |
| [c] The operational incident-handling capability includes detection. | No Answer |
| [d] The operational incident-handling capability includes analysis. | No Answer |
| [e] The operational incident-handling capability includes containment. | No Answer |
| [f] The operational incident-handling capability includes recovery. | No Answer |
| [g] The operational incident-handling capability includes user response activities. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f]  [g] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f]  [g] | |

|  |  |
| --- | --- |
| IR.L2-3.6.2 | Incident Reporting (IR.L2-3.6.2) | |
| Main Control Description: Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Incidents are tracked. | No Answer |
| [b] Incidents are documented. | No Answer |
| [c] Authorities to whom incidents are to be reported are identified. | No Answer |
| [d] Organizational officials to whom incidents are to be reported are identified. | No Answer |
| [e] Identified authorities are notified of incidents. | No Answer |
| [f] Identified organizational officials are notified of incidents. | No Answer |
| Implementation Details:  There is no formal tool to track incidents, and nothing is documented. Information is captured from one-on-one sessions. JIRACOR has an IRP.  [a]  [b]  [c]  [d]  [e]  [f] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f] | |

|  |  |
| --- | --- |
| IR.L2-3.6.3 | Incident Response Testing (IR.L2-3.6.3) | |
| Main Control Description: Test the organizational incident response capability. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if the incident response capability is tested. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| C007 | Maintenance (MA) |
| Maintenance activities are critical to maintaining the technology assets that support or process CUI is maintained for operational sustainment and protection of sensitive data. | |

|  |  |
| --- | --- |
| MA.L2-3.7.1 | Perform Maintenance (MA.L2-3.7.1) | |
| Main Control Description: Perform maintenance on organizational systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if system maintenance is performed. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| MA.L2-3.7.2 | System Maintenance Control (MA.L2-3.7.2) | |
| Main Control Description: Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Tools used to conduct system maintenance are controlled. | No Answer |
| [b] Techniques used to conduct system maintenance are controlled. | No Answer |
| [c] Mechanisms used to conduct system maintenance are controlled. | No Answer |
| [d] Personnel used to conduct system maintenance are controlled. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| MA.L2-3.7.3 | Equipment Sanitization (MA.L2-3.7.3) | |
| Main Control Description: Ensure equipment removed for off-site maintenance is sanitized of any CU. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI. | No Answer |
| Implementation Details:  Equipment is sanitized. | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| MA.L2-3.7.4 | Media Inspection (MA.L2-3.7.4) | |
| Main Control Description: Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| MA.L2-3.7.5 | Nonlocal Maintenance (MA.L2-3.7.5) | |
| Main Control Description: Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Multifactor authentication is used to establish nonlocal maintenance sessions via external network connections. | No Answer |
| [b] Nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| MA.L2-3.7.6 | Maintenance Personnel (MA.L2-3.7.6) | |
| Main Control Description: Supervise the maintenance activities of personnel without required access authorization. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if maintenance personnel without required access authorization are supervised during maintenance activities. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| C008 | Media Protection (MP) |
| Media Protection activities ensure media used to store or transport CUI is identified and protected in accordance with defined requirements. | |

|  |  |
| --- | --- |
| MP.L2-3.8.1 | Media Protection (MP.L2-3.8.1) | |
| Main Control Description: Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Paper media containing CUI is physically controlled. | No Answer |
| [b] Digital media containing CUI is physically controlled. | No Answer |
| [c] Paper media containing CUI is securely stored. | No Answer |
| [d] Digital media containing CUI is securely stored. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| MP.L2-3.8.2 | Media Access (MP.L2-3.8.2) | |
| Main Control Description: Limit access to CUI on system media to authorized users. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if access to CUI on system media is limited to authorized users. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| MP.L1-3.8.3 | Media Disposal (MP.L1-3.8.3) | |
| Main Control Description: Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] System media containing CUI is sanitized or destroyed before disposal. | No Answer |
| [b] System media containing CUI is sanitized before it is released for reuse. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| MP.L2-3.8.4 | Media Markings (MP.L2-3.8.4) | |
| Main Control Description: Mark media with necessary CUI markings and distribution limitations. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Media containing CUI is marked with applicable CUI markings. | No Answer |
| [b] Media containing CUI is marked with distribution limitations. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| MP.L2-3.8.5 | Media Accountability (MP.L2-3.8.5) | |
| Main Control Description: Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Access to media containing CUI is controlled. | No Answer |
| [b] Accountability for media containing CUI is maintained during transport outside of controlled areas. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| MP.L2-3.8.6 | Portable Storage Encryption (MP.L2-3.8.6) | |
| Main Control Description: Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| MP.L2-3.8.7 | Removable Media (MP.L2-3.8.7) | |
| Main Control Description: Control the use of removable media on system components. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if the use of removable media on system components is controlled. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| MP.L2-3.8.8 | Shared Media (MP.L2-3.8.8) | |
| Main Control Description: Prohibit the use of portable storage devices when such devices have no identifiable owner. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if the use of portable storage devices is prohibited when such devices have no identifiable owner. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| MP.L2-3.8.9 | Protect Backups (MP.L2-3.8.9) | |
| Main Control Description: Protect the confidentiality of backup CUI at storage locations. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if the confidentiality of backup CUI is protected at storage locations. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| C009 | Personnel Security (PS) |
| Personnel Security activities are concerned with developing processes to ensure personnel are adequately vetted for the performance of their assigned roles that require access to CUI. | |

|  |  |
| --- | --- |
| PS.L2-3.9.1 | Screen Individuals (PS.L2-3.9.1) | |
| Main Control Description: Screen individuals prior to authorizing access to organizational systems containing CUI. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if individuals are screened prior to authorizing access to organizational systems containing CUI. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| PS.L2-3.9.2 | Personnel Actions (PS.L2-3.9.2) | |
| Main Control Description: Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] A policy and/or process for terminating system access and any credentials coincident with personnel actions is established. | No Answer |
| [b] System access and credentials are terminated consistent with personnel actions such as termination or transfer. | No Answer |
| [c] The system is protected during and after personnel transfer actions. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| C010 | Physical Protection (PE) |
| Physical Protection activities ensure that physical access to CUI asset containers is strictly controlled, managed, and monitored in accordance with CUI protection requirements. | |

|  |  |
| --- | --- |
| PE.L1-3.10.1 | Limit Physical Access (PE.L1-3.10.1) | |
| Main Control Description: Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Authorized individuals allowed physical access are identified. | No Answer |
| [b] Physical access to organizational systems is limited to authorized individuals. | No Answer |
| [c] Physical access to equipment is limited to authorized individuals. | No Answer |
| [d] Physical access to operating environments is limited to authorized individuals. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| PE.L2-3.10.2 | Monitor Facility (PE.L2-3.10.2) | |
| Main Control Description: Protect and monitor the physical facility and support infrastructure for organizational systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The physical facility where organizational systems reside is protected. | No Answer |
| [b] The support infrastructure for organizational systems is protected. | No Answer |
| [c] The physical facility where organizational systems reside is monitored. | No Answer |
| [d] The support infrastructure for organizational systems is monitored. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d] | |
| Objective Evidence:  [a]  [b]  [c]  [d] | |

|  |  |
| --- | --- |
| PE.L1-3.10.3 | Escort Visitors (PE.L1-3.10.3) | |
| Main Control Description: Escort visitors and monitor visitor activity. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Visitors are escorted. | No Answer |
| [b] Visitor activity is monitored. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| PE.L1-3.10.4 | Physical Access Logs (PE.L1-3.10.4) | |
| Main Control Description: Maintain audit logs of physical access. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if audit logs of physical access are maintained. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| PE.L1-3.10.5 | Manage Physical Access (PE.L1-3.10.5) | |
| Main Control Description: Control and manage physical access devices. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Physical access devices are identified. | No Answer |
| [b] Physical access devices are controlled. | No Answer |
| [c] Physical access devices are managed. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| PE.L2-3.10.6 | Alternative Work Sites (PE.L2-3.10.6) | |
| Main Control Description: Enforce safeguarding measures for CUI at alternate work sites. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Safeguarding measures for CUI are defined for alternate work sites. | No Answer |
| [b] Safeguarding measures for CUI are enforced for alternate work sites. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| C011 | Risk Assessment (RA) |
| Cybersecurity risk is defined as risk to organizational operations, resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information or IT. Cybersecurity risk cannot be completely eliminated, but it can be managed through informed decision-making processes. The totality of the CMMC practices serve to manage risk. Practices captured here include specific risk mitigation focused practices such as risk identification and planning. | |

|  |  |
| --- | --- |
| RA.L2-3.11.1 | Risk Assessments (RA.L2-3.11.1) | |
| Main Control Description: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The frequency to assess risk to organizational operations, organizational assets, and individuals is defined. | No Answer |
| [b] Risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| RA.L2-3.11.2 | Vulnerability Scan (RA.L2-3.11.2) | |
| Main Control Description: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The frequency to scan for vulnerabilities in organizational systems and applications is defined. | No Answer |
| [b] Vulnerability scans are performed on organizational systems with the defined frequency. | No Answer |
| [c] Vulnerability scans are performed on applications with the defined frequency. | No Answer |
| [d] Vulnerability scans are performed on organizational systems when new vulnerabilities are identified. | No Answer |
| [e] Vulnerability scans are performed on applications when new vulnerabilities are identified. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e] | |

|  |  |
| --- | --- |
| RA.L2-3.11.3 | Vulnerability Remediation (RA.L2-3.11.3) | |
| Main Control Description: Remediate vulnerabilities in accordance with risk assessments. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Vulnerabilities are identified. | No Answer |
| [b] Vulnerabilities are remediated in accordance with risk assessments. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| C012 | Security Assessment (CA) |
| A security assessment program manages the development and implementation of defined security requirements through the development of a system security plan. A system security plan has the information an organization needs to design and implement solutions that comply with the organization's defined security requirements. | |

|  |  |
| --- | --- |
| CA.L2-3.12.1 | Security Control Assessment (CA.L2-3.12.1) | |
| Main Control Description: Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The frequency of security control assessments is defined. | No Answer |
| [b] Security controls are assessed with the defined frequency to determine if the controls are effective in their application. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| CA.L2-3.12.2 | Plan of Action (CA.L2-3.12.2) | |
| Main Control Description: Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Deficiencies and vulnerabilities to be addressed by the plan of action are identified. | No Answer |
| [b] A plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities. | No Answer |
| [c] The plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| CA.L2-3.12.3 | Security Control Monitoring (CA.L2-3.12.3) | |
| Main Control Description: Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| CA.L2-3.12.4 | System Security Plan (CA.L2-3.12.4) | |
| Main Control Description: Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] A system security plan is developed. | No Answer |
| [b] The system boundary is described and documented in the system security plan. | No Answer |
| [c] The system environment of operation is described and documented in the system security plan. | No Answer |
| [d] The security requirements identified and approved by the designated authority as non-applicable are identified. | No Answer |
| [e] The method of security requirement implementation is described and documented in the system security plan. | No Answer |
| [f] The relationship with or connection to other systems is described and documented in the system security plan. | No Answer |
| [g] The frequency to update the system security plan is defined. | No Answer |
| [h] System security plan is updated with the defined frequency. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f]  [g]  [h] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f]  [g]  [h] | |

|  |  |
| --- | --- |
| C013 | System and Communications Protection (SC) |
| System and Communications Protection activities ensure the organization is actively identifying, managing, and controlling all system and communication channels that store or transit CUI. | |

|  |  |
| --- | --- |
| SC.L1-3.13.1 | Boundary Protection (SC.L1-3.13.1) | |
| Main Control Description: 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 information systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The external system boundary is defined. | No Answer |
| [b] Key internal system boundaries are defined. | No Answer |
| [c] Communications are monitored at the external system boundary. | No Answer |
| [d] Communications are monitored at key internal boundaries. | No Answer |
| [e] Communications are controlled at the external system boundary. | No Answer |
| [f] Communications are controlled at key internal boundaries. | No Answer |
| [g] Communications are protected at the external system boundary. | No Answer |
| [h] Communications are protected at key internal boundaries. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f]  [g]  [h] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f]  [g]  [h] | |

|  |  |
| --- | --- |
| SC.L2-3.13.2 | Security Engineering (SC.L2-3.13.2) | |
| Main Control Description: Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Architectural designs that promote effective information security are identified. | No Answer |
| [b] Software development techniques that promote effective information security are identified. | No Answer |
| [c] Systems engineering principles that promote effective information security are identified. | No Answer |
| [d] Identified architectural designs that promote effective information security are employed. | No Answer |
| [e] Identified software development techniques that promote effective information security are employed. | No Answer |
| [f] Identified systems engineering principles that promote effective information security are employed. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f] | |

|  |  |
| --- | --- |
| SC.L2-3.13.3 | Role Separation (SC.L2-3.13.3) | |
| Main Control Description: Separate user functionality from system management functionality. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] User functionality is identified. | No Answer |
| [b] System management functionality is identified. | No Answer |
| [c] User functionality is separated from system management functionality. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| SC.L2-3.13.4 | Shared Resource Control (SC.L2-3.13.4) | |
| Main Control Description: Prevent unauthorized and unintended information transfer via shared system resources. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if unauthorized and unintended information transfer via shared system resources is prevented. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| SC.L1-3.13.5 | Public-Access System Separation (SC.L1-3.13.5) | |
| Main Control Description: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Publicly accessible system components are identified. | No Answer |
| [b] Subnetworks for publicly accessible system components are physically or logically separated from internal networks. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| SC.L2-3.13.6 | Network Communication by Exception (SC.L2-3.13.6) | |
| Main Control Description: Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Network communications traffic is denied by default. | No Answer |
| [b] Network communications traffic is allowed by exception. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| SC.L2-3.13.7 | Split Tunneling (SC.L2-3.13.7) | |
| Main Control Description: 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) | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling). | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| SC.L2-3.13.8 | Data in Transit (SC.L2-3.13.8) | |
| Main Control Description: Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified. | No Answer |
| [b] Alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified. | No Answer |
| [c] Either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| SC.L2-3.13.9 | Connections Termination (SC.L2-3.13.9) | |
| Main Control Description: Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] A period of inactivity to terminate network connections associated with communications sessions is defined. | No Answer |
| [b] Network connections associated with communications sessions are terminated at the end of the sessions. | No Answer |
| [c] Network connections associated with communications sessions are terminated after the defined period of inactivity. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| SC.L2-3.13.10 | Key Management (SC.L2-3.13.10) | |
| Main Control Description: Establish and manage cryptographic keys for cryptography employed in organizational systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Cryptographic keys are established whenever cryptography is employed. | No Answer |
| [b] Cryptographic keys are managed whenever cryptography is employed. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| SC.L2-3.13.11 | CUI Encryption (SC.L2-3.13.11) | |
| Main Control Description: Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| SC.L2-3.13.12 | Collaborative Device Control (SC.L2-3.13.12) | |
| Main Control Description: Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Collaborative computing devices are identified. | No Answer |
| [b] Collaborative computing devices provide indication to users of devices in use. | No Answer |
| [c] Remote activation of collaborative computing devices is prohibited. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| SC.L2-3.13.13 | Mobile Code (SC.L2-3.13.13) | |
| Main Control Description: Control and monitor the use of mobile code. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Use of mobile code is controlled. | No Answer |
| [b] Use of mobile code is monitored. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| SC.L2-3.13.14 | Voice over Internet Protocol (SC.L2-3.13.14) | |
| Main Control Description: Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Use of Voice over Internet Protocol (VoIP) technologies is controlled. | No Answer |
| [b] Use of Voice over Internet Protocol (VoIP) technologies is monitored. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| SC.L2-3.13.15 | Communications Authenticity (SC.L2-3.13.15) | |
| Main Control Description: Protect the authenticity of communications sessions. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if the authenticity of communications sessions is protected. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| SC.L2-3.13.16 | Data at Rest (SC.L2-3.13.16) | |
| Main Control Description: Protect the confidentiality of CUI at rest. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if the confidentiality of CUI at rest is protected. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| C014 | System and Information Integrity (SI) |
| System and Information Integrity activities ensure that technology assets (e.g., desktops, software) that contain CUI are continuously monitored to detect violations of the authorized security state. Additionally, electronic mail (e-mail), a common attack vector, is monitored and protected to detect malicious activity. | |

|  |  |
| --- | --- |
| SI.L1-3.14.1 | Flaw Remediation (SI.L1-3.14.1) | |
| Main Control Description: Identify, report, and correct information system flaws in a timely manner. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The time within which to identify system flaws is specified. | No Answer |
| [b] System flaws are identified within the specified time frame. | No Answer |
| [c] The time within which to report system flaws is specified. | No Answer |
| [d] System flaws are reported within the specified time frame. | No Answer |
| [e] The time within which to correct system flaws is specified. | No Answer |
| [f] System flaws are corrected within the specified time frame. | No Answer |
| Implementation Details:  [a]  [b]  [c]  [d]  [e]  [f] | |
| Objective Evidence:  [a]  [b]  [c]  [d]  [e]  [f] | |

|  |  |
| --- | --- |
| SI.L1-3.14.2 | Malicious Code Protection (SI.L1-3.14.2) | |
| Main Control Description: Provide protection from malicious code at appropriate locations within organizational information systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Designated locations for malicious code protection are identified. | No Answer |
| [b] Protection from malicious code at designated locations is provided. | No Answer |
| Implementation Details:  Windows Defender, Malwarebytes, automated scans.  Need a defined policy for malicious code protection. No ATP for Windows Defender  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

|  |  |
| --- | --- |
| SI.L2-3.14.3 | Security Alerts & Advisories (SI.L2-3.14.3) | |
| Main Control Description: Monitor system security alerts and advisories and take action in response. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Response actions to system security alerts and advisories are identified. | No Answer |
| [b] System security alerts and advisories are monitored. | No Answer |
| [c] Actions in response to system security alerts and advisories are taken. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| SI.L1-3.14.4 | Update Malicious Code Protection (SI.L1-3.14.4) | |
| Main Control Description: Update malicious code protection mechanisms when new releases are available. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| Determine if malicious code protection mechanisms are updated when new releases are available. | No Answer |
| Implementation Details: N/A | |
| Objective Evidence: | |

|  |  |
| --- | --- |
| SI.L1-3.14.5 | System & File Scanning (SI.L1-3.14.5) | |
| Main Control Description: Perform periodic scans of information systems and real-time scans of files from external sources as files are downloaded, opened, or executed. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The frequency for malicious code scans is defined. | No Answer |
| [b] Malicious code scans are performed with the defined frequency. | No Answer |
| [c] Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| SI.L2-3.14.6 | Monitor Communications for Attacks (SI.L2-3.14.6) | |
| Main Control Description: Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] The system is monitored to detect attacks and indicators of potential attacks. | No Answer |
| [b] Inbound communications traffic is monitored to detect attacks and indicators of potential attacks. | No Answer |
| [c] Outbound communications traffic is monitored to detect attacks and indicators of potential attacks. | No Answer |
| Implementation Details:  [a]  [b]  [c] | |
| Objective Evidence:  [a]  [b]  [c] | |

|  |  |
| --- | --- |
| SI.L2-3.14.7 | Identify Unauthorized Use (SI.L2-3.14.7) | |
| Main Control Description: Identify unauthorized use of organizational systems. | |
| Main Control Implementation Status: ⬜️ Met ⬜️ Partially Met ⬜️ Not Met ⬜️ Not Applicable | |
| Objective Criteria | Status |
| [a] Authorized use of the system is defined. | No Answer |
| [b] Unauthorized use of the system is identified. | No Answer |
| Implementation Details:  [a]  [b] | |
| Objective Evidence:  [a]  [b] | |

# **9. System Security Plan Approvals**

|  |  |
| --- | --- |
| Signature | |
| Name |  |
| Title |  |
| Organization |  |
| Date |  |
| Signature |  |

Prepared By

| Organization that prepared this document | |
| --- | --- |
| Organization Name | Alluvionic Inc. |
| Street Address |  |
| Suite/Room/Building |  |
| City, State Zip code |  |

Prepared For

| Organization | |
| --- | --- |
| Organization Name | [INSERT COMPANY NAME] |
| Street Address |  |
| Suite/Room/Building |  |
| City, State Zip code |  |