|  |
| --- |
| <<Company>>NIST SP 800-171 System Security Plan (SSP)As ofdd mmm yyyyVersion x.x |

Record of Acceptance/Approval

|  |
| --- |
| **System Security Officer** |
| Printed Name: **<Insert Name>** | Date:  |
| Signature: | <MM/DD/YYYY> |

|  |
| --- |
| **Information System Security Officer** |
| Printed Name: **<Insert Name>** | Date:  |
| Signature: | <MM/DD/YYYY> |

Table of Contents

[1 Purpose 4](#_Toc139285576)

[2 Scope 4](#_Toc139285577)

[3 References 4](#_Toc139285578)

[4 Roles & Responsibilities 4](#_Toc139285579)

[5 System Information 4](#_Toc139285580)

[5.1 Responsible Organization 5](#_Toc139285581)

[5.2 Government Information Owner Contact Information 5](#_Toc139285582)

[5.3 System Owner 5](#_Toc139285583)

[5.4 System Security Officer: 5](#_Toc139285584)

[5.5 General Description/Purpose of System: 5](#_Toc139285585)

[5.6 General Description of Information: 6](#_Toc139285586)

[6 System Environment 6](#_Toc139285587)

[6.1 CUI Data Flow Diagrams 6](#_Toc139285588)

[6.1.1 Data Flow Diagram Legend 7](#_Toc139285589)

[6.2 CUI Repositories 7](#_Toc139285590)

[6.3 System Description 7](#_Toc139285591)

[6.3.1 CUI Components 7](#_Toc139285592)

[6.3.2 Security Protection Components 7](#_Toc139285593)

[6.3.3 Out-of-Scope 8](#_Toc139285594)

[6.4 Networking Diagrams 8](#_Toc139285595)

[6.4.1 On-premises Topology 8](#_Toc139285596)

[6.4.2 On-premises Logical Segments 8](#_Toc139285597)

[6.4.3 Azure GCCH Logical Topology 8](#_Toc139285598)

[6.4.4 Zone-to-Zone Communication Tracking 8](#_Toc139285599)

[6.5 Protecting the Confidentiality of CUI in Transit 8](#_Toc139285600)

[6.6 System Interconnections 8](#_Toc139285601)

[6.7 Hardware and Software Information 8](#_Toc139285602)

[6.8 Related Organization Defined Parameters (ODP) and Procedures 8](#_Toc139285603)

[6.8.1 ODPs 8](#_Toc139285604)

[6.8.2 Procedures 8](#_Toc139285605)

[6.9 System Conformity 9](#_Toc139285606)

[6.9.1 Non-Applicable Items 9](#_Toc139285607)

[7 Organizational Responsibilities 9](#_Toc139285608)

[8 Enforcement 9](#_Toc139285609)

[9 Exception To Policy 9](#_Toc139285610)

[10 Non-Compliance 9](#_Toc139285611)

[Appendix A. Revision History 10](#_Toc139285612)

[Appendix B. NIST SP 800-171 Conformity 11](#_Toc139285613)

[DOCUMENT TRACEABILITY MATRIX (DTM) USAGE 11](#_Toc139285614)

[Access Control [AC] Family 12](#_Toc139285615)

[Awareness & Training [AT] Family 34](#_Toc139285616)

[Audit & Accountability [AU] Family 37](#_Toc139285617)

[Configuration Management [CM] Family 46](#_Toc139285618)

[Identification & Authentication [IA] Family 56](#_Toc139285619)

[Incident Response [IR] Family 67](#_Toc139285620)

[Maintenance [MA] Family 70](#_Toc139285621)

[Media Protection [MP] Family 76](#_Toc139285622)

[Personnel Security [PS] Family 85](#_Toc139285623)

[Physical Environment [PE] Family 87](#_Toc139285624)

[Risk Assessment [RA] Family 93](#_Toc139285625)

[Security Assessment [CA] Family 96](#_Toc139285626)

[System and Communications Protection [SC] Family 100](#_Toc139285627)

[System and Information Integrity [SI] Family 116](#_Toc139285628)

[Appendix C. Non-Federal Organization Controls 123](#_Toc139285629)

[Access Control [AC] Family 123](#_Toc139285630)

[Awareness & Training [AT] Family 123](#_Toc139285631)

[Audit and Accountability [AU] Family 123](#_Toc139285632)

[Assessment, Authorization, and Monitoring [CA] Family 123](#_Toc139285633)

[Configuration Management [CM] Family 124](#_Toc139285634)

[Identification and Authentication [IA] Family 124](#_Toc139285635)

[Incident Response [IR] Family 125](#_Toc139285636)

[Maintenance [MA] Family 125](#_Toc139285637)

[Media Protection [MP] Family 125](#_Toc139285638)

[Physical and Environmental Protection [PE] Family 125](#_Toc139285639)

[Planning [PL] Family 126](#_Toc139285640)

[Personnel Security [PS] Family 126](#_Toc139285641)

[Risk Assessment [RA] Family 127](#_Toc139285642)

[System and Services Acquisition [SA] Family 127](#_Toc139285643)

[System and Communications Protection [SC] Family 128](#_Toc139285644)

[System and Information Integrity [SI] Family 129](#_Toc139285645)

[Appendix D. System Interconnection Matrix 130](#_Toc139285646)

[Appendix E. Organization Information Security Responsibilities 131](#_Toc139285647)

[Appendix F. Overall DFARS Clause 252.204-7012 Compliance 137](#_Toc139285648)

[Appendix G. Related Security Requirements 138](#_Toc139285649)

Table of Figures

[Figure 1. Data Flow Diagram Legend 7](#_Toc139285650)

[Figure 7. System Boundaries 7](#_Toc139285651)

[Figure 8. On-premises Physical Topology 8](#_Toc139285652)

[Figure 8. On-premises Logical Topology 8](#_Toc139285653)

[Figure 8. On-premises Logical Topology 8](#_Toc139285654)

[Figure 11. <<Company>> Organization Chart 9](#_Toc139285655)

Table of Tables

[Table 1. Responsible Organization 5](#_Toc139285656)

[Table 2. System Owner 5](#_Toc139285657)

[Table 3. System Security Officer 5](#_Toc139285658)

[Table 4. System User Counts 5](#_Toc139285659)

[Table 5. Types of CUI Processed, Stored, and Transmitted 6](#_Toc139285660)

[Table 6. Not-Applicable Requirements 9](#_Toc139285661)

[Table 7. Sample Document Trackability Matrix (DTM) 11](#_Toc139285662)

[Table 8. System Interconnection Matrix 130](#_Toc139285663)

[Table 9. Information Security Responsibilities Matrix 131](#_Toc139285664)

[Table 10. Overall DFARS Clause 252.204-7012 Compliance 137](#_Toc139285665)

[Table 11. Related Security Requirements 138](#_Toc139285666)

[Instructions: You will find instructions in this font and color throughout the document. Remove before publication]

# Purpose

The purpose of this System Security Plan (SSP) is to document how <<Company>> (a.k.a., the organization) intends to securely provide an operating environment to support normal commercial clients and those clients who support the United States Defense Industrial Base.

This SSP is not meant to exhaustively document how the organization has implemented Information Security procedures and technical controls to meet regulatory requirements. This plan should be used in conjunction with the information documented in the organization’s other policies, plans, procedures, Organization Defined Parameters (ODP), and Configuration Items (CI) to completely understand how the system is configured.

The organization maintains a <<Company>> Document Traceability Matrix to capture correlations between these components.

# Scope

Except as specified in the plan for out-of-scope portions, this plan applies to the entire organization.

# References

* Federal Information Security Modernization Act (FISMA) of 2014
* 32 Code of Federal Regulations (CFR) Part 117 – National Industrial Security Program Operating manual (NISPOM)
* 32 CFR Part 2002 - Controlled Unclassified Information (CUI)
* 48 CFR §52.204-21 - Basic Safeguarding of Covered Contractor Information Systems
* Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations
* NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
* NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
* Cybersecurity Maturity Model Certification (CMMC) Model and related documentation
* International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, Information Security Management Systems
* Document Traceability Matrix
* <<Company>> Overarching Information Security Policy
* <<Company>> Information Security Risk Management Policy
* <<Company>> Document Traceability Matrix

# Roles & Responsibilities

|  |  |
| --- | --- |
| Chief Executive Officer (CEO) | * Ensure the requirements and resources required in the plan are provided
* Ensure execution of the of the organization related goals and objectives
 |
| Chief Financial Officer | * Ensure the organization’s budget accounts for CMMC consulting, Conformity Assessment, and commercial client support operating costs
 |
| Chief Information Security Officer (CISO) | * Oversee implementation of this Plan
* Update this plan as needed
* Review this plan no less than every year for updates
 |
| Chief Operating Officer | * Comply with the requirements identified in this plan
 |

# System Information

|  |  |
| --- | --- |
| **System Name/Title:** | <<Company>> Controlled Unclassified Information (CUI) Operating Environment |
| **System Categorization:** | High Impact for Confidentiality |
| **System Unique Identifier:** | <<Company>> |

The system is classified as High due to the potential exposure to client Export Controlled information.

## Responsible Organization

Table 1. Responsible Organization

|  |  |
| --- | --- |
| **Name:** | <<Company>> |
| **Address:** |  |
| **Phone:** |  |
| **Cage Code:** |  | **DUNS Number:** |  |

## Government Information Owner Contact Information

Tables to identify the name, title, address, and contact information for the Government Information owner will be updated pending further guidance from CMMC AB.

## System Owner

Table 2. System Owner

|  |  |
| --- | --- |
| **Name:** |  |
| **Title:** |  |
| **Office Address:** |  |
| **Work Phone:** |  |
| **e-Mail Address:** |  |

## System Security Officer:

Table 3. System Security Officer

|  |  |
| --- | --- |
| **Name:** |  |
| **Title:** |  |
| **Office Address:** |  |
| **Work Phone:** |  |
| **e-Mail Address:** |  |

## General Description/Purpose of System:

The purpose of the system is to provide a secure operating environment for the organization to store, process, and transmit CUI and other sensitive information types in support of client consulting services and for Cybersecurity maturity Model Certification (CMMC) Conformation Assessment efforts.

Table 4. System User Counts

|  |  |  |
| --- | --- | --- |
| Role | # Users | # Privileged Users |
| **Organizational Staff** | 1 | 1 |

## General Description of Information:

The organization’s policy is client CUI should never be allowed in the organization’s system.

The organization’s intention is to only process information that is to be treated as CUI at this time in support of Conformity Assessments. Should the Department of Defense or another Federal agency require the organization to declare all related artifacts CUI, the organization is ready to declare content it creates as CUI. The organization recognizes client contamination events of other CUI Categories may occur.

The system is currently designed to support the following CUI Categories:

Table 5. Types of CUI Processed, Stored, and Transmitted

|  |  |
| --- | --- |
| Organizational Index Grouping | CUI Categories |
| Defense | * [Controlled Technical Information](https://www.archives.gov/cui/registry/category-detail/controlled-technical-info)
 |
| Export Control | * [Export Controlled](https://www.archives.gov/cui/registry/category-detail/export-control)
* [Export Controlled Research](https://www.archives.gov/cui/registry/category-detail/export-controlled-research)
 |
| Proprietary Business Information | * [General Proprietary Business Information](https://www.archives.gov/cui/registry/category-detail/proprietary-business-info)
 |

The organization classifies internal sensitive information (a.k.a., Proprietary Business Information) as Confidential & Privileged Information (CPI).

Because the organization may be exposed to Export Controlled CUI, the organization only uses Federal Risk and Authorization Management Program (FedRAMP) High Cloud Service Providers for the processing, storing, and transmitting of CUI.

# System Environment

The organization seeks to continually improve its overall security posture by implementing a Zero-Trust Architecture (ZTA). The following ZTA tenets[[1]](#footnote-2) are followed to continually protect the system:

* All data sources and computing services are considered resources. A network may be composed of multiple classes of devices.
* All communication is secured regardless of network location.
* Access to individual enterprise resources is granted on a per-session basis.
* Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
* The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
* All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
* The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

## CUI Data Flow Diagrams

The following diagrams capture the notional flow of information to-be protected as if it is CUI \_\_\_\_\_\_\_.

### Data Flow Diagram Legend

The following data flow diagrams use a common swim lane-based business process diagramming notation. Of note is where the organization expects to interact with client CUI.

Figure 1. Data Flow Diagram Legend

## CUI Repositories

Identify all locations where CUI is housed

## System Description



Provide a system description with scoping diagram

Figure 2. System Scoping diagram

### CUI Components

#### CUI Assets

Describe the CUI Assets

##### Roles

* Role Title: Describe the role that has access to CUI

##### Facilities

* Facility Controlled Area: Describe the Facility Controlled Area that is used to process or store to CUI

##### Technologies

* Component Name: Describe the technical component used to process, store, or transmit CUI

#### Contractor Risk Managed Assets

Describe the CRMAs

##### Roles

* Role Title: Describe the role that has potential access to CUI as a CRMA

##### Facilities

* Facility Controlled Area: Describe the Facility Controlled Area that is used to process or store to CUI as a CRMA

##### Technologies

* Component Name: Describe the technical component used to process, store, or transmit CUI as a CRMA

#### CUI Specialized Assets

Describe the Specialized Assets

##### Roles

* Role Title: Describe the role that has potential access to CUI using a specialized asset

##### Facilities

* Facility Controlled Area: Describe the Facility Controlled Area that is used to process or store to CUI associated to the specialized asset

##### Technologies

* Component Name: Describe the specialized asset used to process, store, or transmit CUI

### Security Protection Components

Describe the SPAs

#### Security Protection Assets

Describe the SPAs

##### Roles

* Role Title: Describe the role involved in protecting CUI

##### Facilities

* Facility Controlled Area: Describe the Facility Controlled Area that are used to protect CUI

##### Technologies

* Component Name: Describe the specialized asset used to protect CUI

#### Security Protection Specialized Assets

Describe the Specialized Assets

##### Technologies

* Component Name: Describe the specialized asset used to protect CUI

### Out-of-Scope

List all out-of scope components and briefly explain why

## Networking Diagrams

### On-premises Topology

Insert network diagrams and describe them

Figure 3. On-premises Physical Topology

### On-premises Logical Segments

Insert network diagrams and describe them

Figure 4. On-premises Logical Topology

### Azure GCCH Logical Topology

Insert Azure network diagrams and describe them

Figure 5. On-premises Logical Topology

### Zone-to-Zone Communication Tracking

A zone-to-zone communication matrix is maintained by the organization and tracked as a Configuration Item.

## Protecting the Confidentiality of CUI in Transit

Describe protection of CUI in transit

## System Interconnections

System interconnections can be found in Appendix E. System Interconnection Matrix.

## Hardware and Software Information

All on-premises hardware are owned by the organization. The organization allows connection of personal devices to the primary CUI repository only after installation of and compliance with the required configurations.

A complete, up-to-date list of in-scope hardware and software is available upon request.

## Related Organization Defined Parameters (ODP) and Procedures

### ODPs

Location of ODPS

### Procedures

Location of procedures

## System Conformity

System Conformity for all CMMC Level 2 and NIST SP 800-171 requirements can be found in Appendix B. NIST SP 800-171 Conformity.

### Non-Applicable Items

The organization determined the following are Not Applicable (N/A) to the system:

Table 6. Not-Applicable Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NIST SP 800-171 | CMMC ID # | Level of Non-Applicability | Requirement | N/A Justification |
| Enter Requirement # for Full or AO for partial | Enter Requirement # for Full or AO for partial | Full if all AOs are n/a.Partial for each n/a AO | List the full requirement if full otherwise list the AO determine if text | Explain why the organization has determined the requirement is n/a |
|  |  |  |  |  |

# Organizational Responsibilities

The following organization chart depicts how the organization is structured.

Insert org chart

Figure 6. <<Company>> Organization Chart

# Enforcement

The <<Company>> Information Security Office team will verify compliance to this plan through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

# Exception To Policy

The CISO is authorized to approve or deny all Information Security Exception to Policy requests for this plan. Any decision by the CISO may be appealed to the CEO. The following business rules apply:

* All appeals will be submitted via e-mail to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
* All appeals will include a reference to the original Information Security Policy request.
* Appeals will begin with the CISO.
* Final appeal authority is the CEO.
* Any appeals that do not follow the Information Security management structure up to the CEO will be automatically rejected.

# Non-Compliance

Any employee found to have violated this plan may be subject to disciplinary action, up to and including termination of employment.

Contractors are subject to having access to all <<Company>> Information systems removed, and the contractor’s firm contacted for replacement.

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Document Version | Document Revision Description and Rationale | Revision Author /Approver |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. NIST SP 800-171 Conformity

This Appendix lists all security requirements identified and approved by the System Owner and provides the general method of security requirement implementation. Operational and technical details are not included to protect the Organization’s Operational Security interests.

Document Traceability Matrix (DTM) Usage

With regards to NIST SP 800-171 Assessment Objective 3.12.4[e], “the method of security requirement implementation is described and documented in the system security plan,” the organization maintains a Document Traceability Matrix (DTM) to correlate documented policies, plans, procedures, ODPs, and CIs against each requirement.  The sum of these artifacts truly describes how and documents the organization’s implementation of the requirement.

The use of the DTM also protects the organization from over-documenting in the SSP and creating an Operational Security risk.

The table below illustrates how the DTM is to be used to understand how the system is documented.

Table 7. Sample Document Trackability Matrix (DTM)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **NIST SP 800-171 #** | **CMMC#** | **Requirement** | **Related Policies** | **Related Plans** | **Related Procedures** | **Related ODPs** | **Related CIs** |
| **3.3.1** | AU.L2-3.3.1  | 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.  | * Audit and Accountability Policy, para 7.1.1, 7.1.3
 | * Audit and Accountability Plan
 | * Change Management Procedures
 | * Audit Log Retention Schedule ODP
 | * 365 Defender | Audit Retention Policy
 |

In the example above, when reviewing NIST SP 800-171 requirement 3.3.1, the DTM provides the user the ability to correlated:

* **Related Policies:**  In the example above, the requirement was taken into consideration during the writing of Audit and Accountability Policy and specifically paragraphs 7.1.1 and 7.1.3
* **Related Plans:**  In this case the requirement is supported by a plan, Audit and Accountability Plan.  Every plan has an imbedded Related Requirements table to further guide the reviewer.
* **Related Procedure(s):** The DTM will list all related known repeatable procedures that are used to implement the requirements.  In this case, the DTM references the Change Management Procedures enumerated in the Configuration Management Plan (CMP).  The Change Management Procedures are used to affect changes to the system and related CIs.
* **Related ODPs:**  ODPs are used to capture where the organization has defined, established, identified, or specified a parameter used to guide how the organization operates.  In this case the DTM points to the Audit Log Retention Schedule ODP.
* **Related CIs:**  This column will list all the related configuration items that are configured on system components to implement the requirement.  In this case, there is a Configuration Item in Microsoft 365 Defender that technically affects how this requirement is implemented.
* **Evidentiary Artifacts:**  For formal audits, the organization will add a supplemental column to list evidentiary artifacts that may be generated as a result of the requirement.  For this requirement, it may be a screenshot of raw audit logs.

Given the number of items and size of the DTM, the DTM will only be provided upon request.

See 3.1.9 as a sample way to complete documenting your conformity.

Access Control [AC] Family

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

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.1 | Practice Name: | Authorized Access Control |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

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

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.2 | Practice Name: | Transaction & Function Control |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.1.3, Control the flow of CUI in accordance with approved authorizations.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.3 | Practice Name: | Control CUI Flow |
| Assessment Objective(s) | AO Conformity |
| [a] information flow control policies are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] methods and enforcement mechanisms for controlling the flow of CUI are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] authorizations for controlling the flow of CUI are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] approved authorizations for controlling the flow of CUI are enforced. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

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

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.4 | Practice Name: | Separation of Duties |
| Assessment Objective(s) | AO Conformity |
| [a] the duties of individuals requiring separation are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] responsibilities for duties that require separation are assigned to separate individuals. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

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

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.5 | Practice Name: | Least Privilege |
| Assessment Objective(s) | AO Conformity |
| [a] privileged accounts are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] access to privileged accounts is authorized in accordance with the principle of least privilege. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] security functions are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] access to security functions is authorized in accordance with the principle of least privilege. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

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

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.6 | Practice Name: | Non-Privileged Account Use |
| Assessment Objective(s) | AO Conformity |
| [a] nonsecurity functions are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] users are required to use non-privileged accounts or roles when accessing nonsecurity functions. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

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

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.7 | Practice Name: | Privileged Functions |
| Assessment Objective(s) | AO Conformity |
| [a] privileged functions are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] non-privileged users are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] non-privileged users are prevented from executing privileged functions. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] the execution of privileged functions is captured in audit logs. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.8, Limit unsuccessful logon attempts.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.8 | Practice Name: | Unsuccessful Logon Attempts |
| Assessment Objective(s) | AO Conformity |
| [a] the means of limiting unsuccessful logon attempts is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] the defined means of limiting unsuccessful logon attempts is implemented. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.9, Provide privacy and security notices consistent with applicable CUI rules.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.9 | Practice Name: | Privacy & Security Notices |
| Assessment Objective(s) | AO Conformity |
| [a] privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:***The organization approved its Notice and Consent banner language on 26 August 2020 and is defines in the Information Security Notebook OneNote file under Organization Defined Parameters > Device Configurations > Notice & Consent Banner. |
|  |
| [b] privacy and security notices are displayed. | [b] privacy and security notices are displayed. |
| ***Assessment Objective Conformity Statement:***The organization uses Microsoft Intune Device Configurations to set the Notice & Consent Banner language for all MacOS and Windows devices. The Notice & Consent banner is also configured for login to Azure and Office 365.The organization could not set the Notice & Consent Banner language for both Cisco Duo and Cisco Umbrella as neither capability provides that functionality. |

3.1.10, Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.10 | Practice Name: | Session Lock |
| Assessment Objective(s) | AO Conformity |
| [a] the period of inactivity after which the system initiates a session lock is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] previously visible information is concealed via a pattern-hiding display after the defined period of inactivity. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.11, Terminate (automatically) a user session after a defined condition.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.11 | Practice Name: | Session Termination |
| Assessment Objective(s) | AO Conformity |
| [a] conditions requiring a user session to terminate are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] a user session is automatically terminated after any of the defined conditions occur. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.12, Monitor and control remote access sessions.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.12 | Practice Name: | Control Remote Access |
| Assessment Objective(s) | AO Conformity |
| [a] remote access sessions are permitted. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] the types of permitted remote access are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] remote access sessions are controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] remote access sessions are monitored. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.13, Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.13 | Practice Name: | Remote Access Confidentiality |
| Assessment Objective(s) | AO Conformity |
| [a] cryptographic mechanisms to protect the confidentiality of remote access sessions are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.14, Route remote access via managed access control points.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.14 | Practice Name: | Remote Access Routing |
| Assessment Objective(s) | AO Conformity |
| [a] managed access control points are identified and implemented. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] remote access is routed through managed network access control points. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.15, Authorize remote execution of privileged commands and remote access to securityrelevant information.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.15 | Practice Name: | Privileged Remote Access |
| Assessment Objective(s) | AO Conformity |
| [a] privileged commands authorized for remote execution are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] security-relevant information authorized to be accessed remotely is identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] the execution of the identified privileged commands via remote access is authorized. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] access to the identified security-relevant information via remote access is authorized. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.16, Authorize wireless access prior to allowing such connections.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.16 | Practice Name: | Wireless Access Authorization |
| Assessment Objective(s) | AO Conformity |
| [a] wireless access points are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] wireless access is authorized prior to allowing such connections. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.17, Protect wireless access using authentication and encryption.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.17 | Practice Name: | Wireless Access Protection |
| Assessment Objective(s) | AO Conformity |
| [a] wireless access to the system is protected using authentication. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] wireless access to the system is protected using encryption. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.18, Control connection of mobile devices.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.18 | Practice Name: | Mobile Device Connection |
| Assessment Objective(s) | AO Conformity |
| [a] mobile devices that process, store, or transmit CUI are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] mobile device connections are authorized. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] mobile device connections are monitored and logged. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.19, Encrypt CUI on mobile devices and mobile computing platforms. [Mobile devices and computing platforms include, for example, smartphones and tablets. 23

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.19 | Practice Name: | Encrypt CUI on Mobile |
| Assessment Objective(s) | AO Conformity |
| [a] mobile devices and mobile computing platforms that process, store, or transmit CUI are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] encryption is employed to protect CUI on identified mobile devices and mobile computing platforms. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.20, Verify and control/limit connections to and use of external systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.20 | Practice Name: | External Connections |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.1.21, Limit use of portable storage devices on external systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.21 | Practice Name: | Portable Storage Use |
| Assessment Objective(s) | AO Conformity |
| [a] the use of portable storage devices containing CUI on external systems is identified and documented. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] limits on the use of portable storage devices containing CUI on external systems are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] the use of portable storage devices containing CUI on external systems is limited as defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.1.22, Control CUI posted or processed on publicly accessible systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AC.L2-3.1.22 | Practice Name: | Control Public Information |
| Assessment Objective(s) | AO Conformity |
| [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 CUI 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 CUI. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] mechanisms are in place to remove and address improper posting of CUI. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Awareness & Training [AT] Family

3.2.1, Ensure that managers, systems 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.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AT.L2-3.2.1 | Practice Name: | Role-Based Risk Awareness |
| Assessment Objective(s) | AO Conformity |
| [a] security risks associated with organizational activities involving CUI are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] policies, standards, and procedures related to the security of the system are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] managers, systems administrators, and users of the system are made aware of the security risks associated with their activities. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [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. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.2.2, Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AT.L2-3.2.2 | Practice Name: | Role-Based Training |
| Assessment Objective(s) | AO Conformity |
| [a] information security-related duties, roles, and responsibilities are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] information security-related duties, roles, and responsibilities are assigned to designated personnel. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.2.3, Provide security awareness training on recognizing and reporting potential indicators of insider threat.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AT.L2-3.2.3 | Practice Name: | Insider Threat Awareness |
| Assessment Objective(s) | AO Conformity |
| [a] potential indicators associated with insider threats are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Audit & Accountability [AU] Family

3.3.1, 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.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AU.L2-3.3.1 | Practice Name: | System Auditing |
| Assessment Objective(s) | AO Conformity |
| [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. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] audit records are created (generated). | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] audit records, once created, contain the defined content. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] retention requirements for audit records are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [f] audit records are retained as defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.3.2, Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AU.L2-3.3.2 | Practice Name: | User Accountability |
| Assessment Objective(s) | AO Conformity |
| [a] the content of the audit records needed to support the ability to uniquely trace users to their actions is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
|  | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:***[b] audit records, once created, contain the defined content. |

3.3.3, Review and update logged events.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AU.L2-3.3.3 | Practice Name: | Event Review |
| Assessment Objective(s) | AO Conformity |
| [a] a process for determining when to review logged events is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] event types being logged are reviewed in accordance with the defined review process. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] event types being logged are updated based on the review. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.3.4, Alert in the event of an audit logging process failure.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AU.L2-3.3.4 | Practice Name: | Audit Failure Alerting |
| Assessment Objective(s) | AO Conformity |
| [a] personnel or roles to be alerted in the event of an audit logging process failure are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] types of audit logging process failures for which alert will be generated are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] identified personnel or roles are alerted in the event of an audit logging process failure. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.3.5, Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AU.L2-3.3.5 | Practice Name: | Audit Correlation |
| Assessment Objective(s) | AO Conformity |
| [a] audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] defined audit record review, analysis, and reporting processes are correlated. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.3.6, Provide audit record reduction and report generation to support on-demand analysis and reporting.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AU.L2-3.3.6 | Practice Name: | Reduction & Reporting |
| Assessment Objective(s) | AO Conformity |
| [a] an audit record reduction capability that supports on-demand analysis is provided. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] a report generation capability that supports on-demand reporting is provided. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.3.7, Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AU.L2-3.3.7 | Practice Name: | Authoritative Time Source |
| Assessment Objective(s) | AO Conformity |
| [a] internal system clocks are used to generate time stamps for audit records. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] an authoritative source with which to compare and synchronize internal system clocks is specified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.3.8, Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AU.L2-3.3.8 | Practice Name: | Audit Protection |
| Assessment Objective(s) | AO Conformity |
| [a] audit information is protected from unauthorized access. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] audit information is protected from unauthorized modification. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] audit information is protected from unauthorized deletion. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] audit logging tools are protected from unauthorized access. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] audit logging tools are protected from unauthorized modification. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [f] audit logging tools are protected from unauthorized deletion. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.3.9, Limit management of audit logging functionality to a subset of privileged users.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | AU.L2-3.3.9 | Practice Name: | Audit Management |
| Assessment Objective(s) | AO Conformity |
| [a] a subset of privileged users granted access to manage audit logging functionality is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] management of audit logging functionality is limited to the defined subset of privileged users. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Configuration Management [CM] Family

3.4.1, Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CM.L2-3.4.1 | Practice Name: | System Baselining |
| Assessment Objective(s) | AO Conformity |
| [a] a baseline configuration is established. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] the baseline configuration includes hardware, software, firmware, and documentation. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] a system inventory is established. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] the system inventory includes hardware, software, firmware, and documentation. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [f] the inventory is maintained (reviewed and updated) throughout the system development life cycle. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.4.2, Establish and enforce security configuration settings for information technology products employed in organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CM.L2-3.4.2 | Practice Name: | Security Configuration Enforcement |
| Assessment Objective(s) | AO Conformity |
| [a] security configuration settings for information technology products employed in the system are established and included in the baseline configuration. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] security configuration settings for information technology products employed in the system are enforced. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.4.3, Track, review, approve or disapprove, and log changes to organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CM.L2-3.4.3 | Practice Name: | System Change Management |
| Assessment Objective(s) | AO Conformity |
| [a] changes to the system are tracked. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] changes to the system are reviewed. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] changes to the system are approved or disapproved. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] changes to the system are logged. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.4.4, Analyze the security impact of changes prior to implementation.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CM.L2-3.4.4 | Practice Name: | Security Impact Analysis |
| Assessment Objective(s) | AO Conformity |
| [a] Determine if the security impact of changes to the system is analyzed prior to implementation. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.4.5, Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CM.L2-3.4.5 | Practice Name: | Access Restrictions for Change |
| Assessment Objective(s) | AO Conformity |
| [a] physical access restrictions associated with changes to the system are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] physical access restrictions associated with changes to the system are documented. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] physical access restrictions associated with changes to the system are approved. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] physical access restrictions associated with changes to the system are enforced. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] logical access restrictions associated with changes to the system are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [f] logical access restrictions associated with changes to the system are documented. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [g] logical access restrictions associated with changes to the system are approved. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
|  |
| [h] logical access restrictions associated with changes to the system are enforced. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.4.6, Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CM.L2-3.4.6 | Practice Name: | Least Functionality |
| Assessment Objective(s) | AO Conformity |
| [a] essential system capabilities are defined based on the principle of least functionality. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] the system is configured to provide only the defined essential capabilities. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.4.7, Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CM.L2-3.4.7 | Practice Name: | Nonessential Functionality |
| Assessment Objective(s) | AO Conformity |
| [a] essential programs are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] the use of nonessential programs is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] the use of nonessential programs is restricted, disabled, or prevented as defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] essential functions are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] the use of nonessential functions is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [f] the use of nonessential functions is restricted, disabled, or prevented as defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [g] essential ports are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [h] the use of nonessential ports is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [i] the use of nonessential ports is restricted, disabled, or prevented as defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [j] essential protocols are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [k] the use of nonessential protocols is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [l] the use of nonessential protocols is restricted, disabled, or prevented as defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [m] essential services are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [n] the use of nonessential services is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [o] the use of nonessential services is restricted, disabled, or prevented as defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.4.8, 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.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CM.L2-3.4.8 | Practice Name: | Application Execution Policy |
| Assessment Objective(s) | AO Conformity |
| [a] a policy specifying whether whitelisting or blacklisting is to be implemented is specified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] the software allowed to execute under whitelisting or denied use under blacklisting is specified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.4.9, Control and monitor user-installed software.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CM.L2-3.4.9 | Practice Name: | User-Installed Software |
| Assessment Objective(s) | AO Conformity |
| [a] a policy for controlling the installation of software by users is established. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] installation of software by users is controlled based on the established policy. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] installation of software by users is monitored. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Identification & Authentication [IA] Family

3.5.1, Identify system users, processes acting on behalf of users, and devices.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.1 | Practice Name: | Identification |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.5.2, Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.2 | Practice Name: | Authentication |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.5.3, Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.3 | Practice Name: | Multifactor Authentication |
| Assessment Objective(s) | AO Conformity |
| [a] privileged accounts are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] multifactor authentication is implemented for local access to privileged accounts. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] multifactor authentication is implemented for network access to privileged accounts. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] multifactor authentication is implemented for network access to non-privileged accounts. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.5.4, Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.4 | Practice Name: | Replay-Resistant Authentication |
| Assessment Objective(s) | AO Conformity |
| [a] Determine if replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.5.5, Prevent reuse of identifiers for a defined period.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.5 | Practice Name: | Identifier Reuse |
| Assessment Objective(s) | AO Conformity |
| [a] a period within which identifiers cannot be reused is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] reuse of identifiers is prevented within the defined period. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.5.6, Disable identifiers after a defined period of inactivity.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.6 | Practice Name: | Identifier Handling |
| Assessment Objective(s) | AO Conformity |
| [a] a period of inactivity after which an identifier is disabled is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] identifiers are disabled after the defined period of inactivity. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.5.7, Enforce a minimum password complexity and change of characters when new passwords are created.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.7 | Practice Name: | Password Complexity |
| Assessment Objective(s) | AO Conformity |
| [a] password complexity requirements are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] password change of character requirements are defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] minimum password complexity requirements as defined are enforced when new passwords are created. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] minimum password change of character requirements as defined are enforced when new passwords are created. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.5.8, Prohibit password reuse for a specified number of generations.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.8 | Practice Name: | Password Reuse |
| Assessment Objective(s) | AO Conformity |
| [a] the number of generations during which a password cannot be reused is specified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] reuse of passwords is prohibited during the specified number of generations. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.5.9, Allow temporary password use for system logons with an immediate change to a permanent password.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.9 | Practice Name: | Temporary Passwords |
| Assessment Objective(s) | AO Conformity |
| [a] Determine if an immediate change to a permanent password is required when a temporary password is used for system logon. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.5.10, Store and transmit only cryptographically-protected passwords.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.10 | Practice Name: | Cryptographically-Protected Passwords |
| Assessment Objective(s) | AO Conformity |
| [a] passwords are cryptographically protected in storage. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] passwords are cryptographically protected in transit. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.5.11, Obscure feedback of authentication information.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IA.L2-3.5.11 | Practice Name: | Obscure Feedback |
| Assessment Objective(s) | AO Conformity |
| [a] Determine if authentication information is obscured during the authentication process. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Incident Response [IR] Family

3.6.1, Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IR.L2-3.6.1 | Practice Name: | Incident Handling |
| Assessment Objective(s) | AO Conformity |
| [a] an operational incident-handling capability is established. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] the operational incident-handling capability includes preparation. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] the operational incident-handling capability includes detection. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] the operational incident-handling capability includes analysis. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] the operational incident-handling capability includes containment. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [f] the operational incident-handling capability includes recovery. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [g] the operational incident-handling capability includes user response activities. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.6.2, Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IR.L2-3.6.2 | Practice Name: | Incident Reporting |
| Assessment Objective(s) | AO Conformity |
| [a] incidents are tracked. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] incidents are documented. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] authorities to whom incidents are to be reported are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] organizational officials to whom incidents are to be reported are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] identified authorities are notified of incidents. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [f] identified organizational officials are notified of incidents. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.6.3, Test the organizational incident response capability.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | IR.L2-3.6.3 | Practice Name: | Incident Response Testing |
| Assessment Objective(s) | AO Conformity |
| [a] Determine if the incident response capability is tested. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Maintenance [MA] Family

3.7.1, Perform maintenance on organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MA.L2-3.7.1 | Practice Name: | Perform Maintenance |
| Assessment Objective(s) | AO Conformity |
| [a] Determine if system maintenance is performed. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.7.2, Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MA.L2-3.7.2 | Practice Name: | System Maintenance Control |
| Assessment Objective(s) | AO Conformity |
| [a] tools used to conduct system maintenance are controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] techniques used to conduct system maintenance are controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] mechanisms used to conduct system maintenance are controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] personnel used to conduct system maintenance are controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.7.3, Ensure equipment removed for off-site maintenance is sanitized of any CUI.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MA.L2-3.7.3 | Practice Name: | Equipment Sanitization |
| Assessment Objective(s) | AO Conformity |
| [a] Determine if equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.7.4, Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MA.L2-3.7.4 | Practice Name: | Media Inspection |
| Assessment Objective(s) | AO Conformity |
| [a] 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. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.7.5, Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MA.L2-3.7.5 | Practice Name: | Nonlocal Maintenance |
| Assessment Objective(s) | AO Conformity |
| [a] multifactor authentication is used to establish nonlocal maintenance sessions via external network connections. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.7.6, Supervise the maintenance activities of maintenance personnel without required access authorization.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MA.L2-3.7.6 | Practice Name: | Maintenance Personnel |
| Assessment Objective(s) | AO Conformity |
| [a] Determine if maintenance personnel without required access authorization are supervised during maintenance activities. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Media Protection [MP] Family

3.8.1, Protect (i.e. physically control and securely store) system media containing CUI, both paper and digital.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MP.L2-3.8.1 | Practice Name: | Media Protection |
| Assessment Objective(s) | AO Conformity |
| [a] paper media containing CUI is physically controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] digital media containing CUI is physically controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] paper media containing CUI is securely stored. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] digital media containing CUI is securely stored. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.8.2, Limit access to CUI on system media to authorized users.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MP.L2-3.8.2 | Practice Name: | Media Access |
| Assessment Objective(s) | AO Conformity |
| [a] access to CUI on system media is limited to authorized users. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.8.3, Sanitize or destroy system media containing CUI before disposal or release for reuse.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MP.L2-3.8.3 | Practice Name: | Media Disposal |
| Assessment Objective(s) | AO Conformity |
| [a] system media containing CUI is sanitized or destroyed before disposal. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] system media containing CUI is sanitized before it is released for reuse. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.8.4, Mark media with necessary CUI markings and distribution limitations.27

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MP.L2-3.8.4 | Practice Name: | Media Markings |
| Assessment Objective(s) | AO Conformity |
| [a] media containing CUI is marked with applicable CUI markings. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] media containing CUI is marked with distribution limitations. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.8.5, Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MP.L2-3.8.5 | Practice Name: | Media Accountability |
| Assessment Objective(s) | AO Conformity |
| [a] access to media containing CUI is controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] accountability for media containing CUI is maintained during transport outside of controlled areas. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.8.6, Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MP.L2-3.8.6 | Practice Name: | Portable Storage Encryption |
| Assessment Objective(s) | AO Conformity |
| [a] the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.8.7, Control the use of removable media on system components.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MP.L2-3.8.7 | Practice Name: | Removable Media |
| Assessment Objective(s) | AO Conformity |
| [a] the use of removable media on system components is controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.8.8, Prohibit the use of portable storage devices when such devices have no identifiable owner.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MP.L2-3.8.8 | Practice Name: | Shared Media |
| Assessment Objective(s) | AO Conformity |
| [a] Determine if the use of portable storage devices is prohibited when such devices have no identifiable owner. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.8.9, Protect the confidentiality of backup CUI at storage locations.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | MP.L2-3.8.9 | Practice Name: | Protect Backups |
| Assessment Objective(s) | AO Conformity |
| [a] the confidentiality of backup CUI is protected at storage locations. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Personnel Security [PS] Family

3.9.1, Screen individuals prior to authorizing access to organizational systems containing CUI.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | PS.L2-3.9.1 | Practice Name: | Screen Individuals |
| Assessment Objective(s) | AO Conformity |
| [a] Determine if individuals are screened prior to authorizing access to organizational systems containing CUI. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.9.2, Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | PS.L2-3.9.2 | Practice Name: | Personnel Actions |
| Assessment Objective(s) | AO Conformity |
| [a] a policy and/or process for terminating system access and any credentials coincident with personnel actions is established. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] system access and credentials are terminated consistent with personnel actions such as termination or transfer. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] the system is protected during and after personnel transfer actions. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Physical Protection [PE] Family

3.10.1, Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | PE.L2-3.10.1 | Practice Name: | Limit Physical Access |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.10.2, Protect and monitor the physical facility and support infrastructure for organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | PE.L2-3.10.2 | Practice Name: | Monitor Facility |
| Assessment Objective(s) | AO Conformity |
| [a] the physical facility where organizational systems reside is protected. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] the support infrastructure for organizational systems is protected. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] the physical facility where organizational systems reside is monitored. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] the support infrastructure for organizational systems is monitored. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.10.3, Escort visitors and monitor visitor activity.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | PE.L2-3.10.3 | Practice Name: | Escort Visitors |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.10.4, Maintain audit logs of physical access.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | PE.L2-3.10.4 | Practice Name: | Physical Access Logs |
| Assessment Objective(s) | AO Conformity |
| [a] audit logs of physical access are maintained. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.10.5, Control and manage physical access devices.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | PE.L2-3.10.5 | Practice Name: | Manage Physical Access |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.10.6, Enforce safeguarding measures for CUI at alternate work sites.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | PE.L2-3.10.6 | Practice Name: | Alternative Work Sites |
| Assessment Objective(s) | AO Conformity |
| [a] safeguarding measures for CUI are defined for alternate work sites. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] safeguarding measures for CUI are enforced for alternate work sites. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Risk Assessment [RA] Family

3.11.1, 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.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | RA.L2-3.11.1 | Practice Name: | Risk Assessments |
| Assessment Objective(s) | AO Conformity |
| [a] the frequency to assess risk to organizational operations, organizational assets, and individuals is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [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. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.11.2, Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | RA.L2-3.11.2 | Practice Name: | Vulnerability Scan |
| Assessment Objective(s) | AO Conformity |
| [a] the frequency to scan for vulnerabilities in organizational systems and applications is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] vulnerability scans are performed on organizational systems with the defined frequency. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] vulnerability scans are performed on applications with the defined frequency. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] vulnerability scans are performed on organizational systems when new vulnerabilities are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] vulnerability scans are performed on applications when new vulnerabilities are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.11.3, Remediate vulnerabilities in accordance with risk assessments.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | RA.L2-3.11.3 | Practice Name: | Vulnerability Remediation |
| Assessment Objective(s) | AO Conformity |
| [a] vulnerabilities are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] vulnerabilities are remediated in accordance with risk assessments. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

Security Assessment [CA] Family

3.12.1, Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CA.L2-3.12.1 | Practice Name: | Security Control Assessment |
| Assessment Objective(s) | AO Conformity |
| [a] the frequency of security control assessments is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] security controls are assessed with the defined frequency to determine if the controls are effective in their application. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.12.2, Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CA.L2-3.12.2 | Practice Name: | Plan of Action |
| Assessment Objective(s) | AO Conformity |
| [a] deficiencies and vulnerabilities to be addressed by the plan of action are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.12.3, Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CA.L2-3.12.3 | Practice Name: | Security Control Monitoring |
| Assessment Objective(s) | AO Conformity |
| [a] security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.12.4, 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.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | CA.L2-3.12.4 | Practice Name: | System Security Plan |
| Assessment Objective(s) | AO Conformity |
| [a] a system security plan is developed. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] the system boundary is described and documented in the system security plan. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] the system environment of operation is described and documented in the system security plan. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] the security requirements identified and approved by the designated authority as non-applicable are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] the method of security requirement implementation is described and documented in the system security plan. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [f] the relationship with or connection to other systems is described and documented in the system security plan. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [g] the frequency to update the system security plan is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [h] system security plan is updated with the defined frequency. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

System and Communications Protection [SC] Family

3.13.1, Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.1 | Practice Name: | Boundary Protection |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.13.2, Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.2 | Practice Name: | Security Engineering |
| Assessment Objective(s) | AO Conformity |
| [a] architectural designs that promote effective information security are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] software development techniques that promote effective information security are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] systems engineering principles that promote effective information security are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [d] identified architectural designs that promote effective information security are employed. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [e] identified software development techniques that promote effective information security are employed. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [f] identified systems engineering principles that promote effective information security are employed. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.3, Separate user functionality from system management functionality.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.3 | Practice Name: | Role Separation |
| Assessment Objective(s) | AO Conformity |
| [a] user functionality is identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] system management functionality is identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] user functionality is separated from system management functionality. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.4, Prevent unauthorized and unintended information transfer via shared system resources.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.4 | Practice Name: | Shared Resource Control |
| Assessment Objective(s) | AO Conformity |
| [a] unauthorized and unintended information transfer via shared system resources is prevented. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.5, Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.5 | Practice Name: | Public-Access System Separation |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.13.6, Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.6 | Practice Name: | Network Communication by Exception |
| Assessment Objective(s) | AO Conformity |
| [a] network communications traffic is denied by default. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] network communications traffic is allowed by exception. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.7, 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).

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.7 | Practice Name: | Split Tunneling |
| Assessment Objective(s) | AO Conformity |
| [a] 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). | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.8, Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.8 | Practice Name: | Data in Transit |
| Assessment Objective(s) | AO Conformity |
| [a] cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.9, Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.9 | Practice Name: | Connections Termination |
| Assessment Objective(s) | AO Conformity |
| [a] a period of inactivity to terminate network connections associated with communications sessions is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] network connections associated with communications sessions are terminated at the end of the sessions. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] network connections associated with communications sessions are terminated after the defined period of inactivity. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.10, Establish and manage cryptographic keys for cryptography employed in organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.10 | Practice Name: | Key Management |
| Assessment Objective(s) | AO Conformity |
| [a] cryptographic keys are established whenever cryptography is employed. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] cryptographic keys are managed whenever cryptography is employed. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.11, Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.11 | Practice Name: | CUI Encryption |
| Assessment Objective(s) | AO Conformity |
| [a] FIPS-validated cryptography is employed to protect the confidentiality of CUI. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.12, Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.12 | Practice Name: | Collaborative Device Control |
| Assessment Objective(s) | AO Conformity |
| [a] collaborative computing devices are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] collaborative computing devices provide indication to users of devices in use. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] remote activation of collaborative computing devices is prohibited. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.13, Control and monitor the use of mobile code.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.13 | Practice Name: | Mobile Code |
| Assessment Objective(s) | AO Conformity |
| [a] use of mobile code is controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] use of mobile code is monitored. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.14, Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.14 | Practice Name: | Voice over Internet Protocol |
| Assessment Objective(s) | AO Conformity |
| [a] use of Voice over Internet Protocol (VoIP) technologies is controlled. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] use of Voice over Internet Protocol (VoIP) technologies is monitored. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.15, Protect the authenticity of communications sessions.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.15 | Practice Name: | Communications Authenticity |
| Assessment Objective(s) | AO Conformity |
| [a] the authenticity of communications sessions is protected. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.13.16, Protect the confidentiality of CUI at rest.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SC.L2-3.13.16 | Practice Name: | Data at Rest |
| Assessment Objective(s) | AO Conformity |
| [a] the confidentiality of CUI at rest is protected. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

System and Information Integrity [SI] Family

3.14.1, Identify, report, and correct system flaws in a timely manner.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SI.L2-3.14.1 | Practice Name: | Flaw Remediation |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.14.2, Provide protection from malicious code at designated locations within organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SI.L2-3.14.2 | Practice Name: | Malicious Code Protection |
| Assessment Objective(s) | AO Conformity |
| [a] designated locations for malicious code protection 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:*** |

3.14.3, Monitor system security alerts and advisories and take action in response.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SI.L2-3.14.3 | Practice Name: | Security Alerts & Advisories |
| Assessment Objective(s) | AO Conformity |
| [a] response actions to system security alerts and advisories are identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] system security alerts and advisories are monitored. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] actions in response to system security alerts and advisories are taken. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.14.4, Update malicious code protection mechanisms when new releases are available.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SI.L2-3.14.4 | Practice Name: | Update Malicious Code Protection |
| Assessment Objective(s) | AO Conformity |
| [a] malicious code protection mechanisms are updated when new releases are available. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.14.5, Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SI.L2-3.14.5 | Practice Name: | System & File Scanning |
| Assessment Objective(s) | AO Conformity |
| [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:*** |

3.14.6, Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SI.L2-3.14.6 | Practice Name: | Monitor Communications for Attacks |
| Assessment Objective(s) | AO Conformity |
| [a] the system is monitored to detect attacks and indicators of potential attacks. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] inbound communications traffic is monitored to detect attacks and indicators of potential attacks. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [c] outbound communications traffic is monitored to detect attacks and indicators of potential attacks. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

3.14.7, Identify unauthorized use of organizational systems.

|  |  |
| --- | --- |
| Requirement Conformity: |  [x]  MET [ ]  NOT MET [ ]  NOT APPLICABLE |
| CMMC Level: | L2 | Practice ID: | SI.L2-3.14.7 | Practice Name: | Identify Unauthorized Use |
| Assessment Objective(s) | AO Conformity |
| [a] authorized use of the system is defined. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |
|  |
| [b] unauthorized use of the system is identified. | [ ]  Met [ ]  Not Met [ ]  N/A |
| ***Assessment Objective Conformity Statement:*** |

1. Plans of Action & Milestones [POA&M]
2. Non-Federal Organization Controls

The following are the Non-Federal Organization (NFO) from NIST SP 800-171, Appendix E, Tailoring Criteria. Per NIST SP 800-171, “The control or control enhancement is expected to be routinely satisfied by nonfederal organizations without specification.” This table is provided for reference only.

The controls below reflect NIST SP 800-53, rev 5.

System and Services Acquisition [SA] Family

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-1  | TITLE: | System and Services Acquisition Policy and Procedures  |
| Description: | System and services acquisition policy and procedures address the controls in the SA family that are implemented within systems and organizations. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-2  | TITLE: | Allocation of Resources  |
| Description: | Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-3  | TITLE: | System Development Life Cycle  |
| Description: | A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions. The security engineering principles in SA-8 help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g., senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers) in system development life cycle processes to ensure that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development life cycle involves multiple organizations, (e.g., external suppliers, developers, integrators, service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-4  | TITLE: | Acquisition Process  |
| Description: | Security and privacy functional requirements are typically derived from the high-level security and privacy requirements described in SA-2. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, and methodologies as well as the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism. [SP 800-160-1] describes the process of requirements engineering as part of the system development life cycle.Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and for reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities. Controls can include technical, administrative, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development life cycle.Security and privacy documentation requirements address all stages of the system development life cycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-4(1)  | TITLE: | ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS |
| Description: | Functional properties of security and privacy controls describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-4(2)  | TITLE: | ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS  |
| Description: | Organizations may require different levels of detail in the documentation for the design and implementation of controls in organizational systems, system components, or system services based on mission and business requirements, requirements for resiliency and trustworthiness, and requirements for analysis and testing. Systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules and the interfaces between modules providing security-relevant functionality. Design and implementation documentation can include manufacturer, version, serial number, verification hash signature, software libraries used, date of purchase or download, and the vendor or download source. Source code and hardware schematics are referred to as the implementation representation of the system. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-4(9)  | TITLE: | ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE  |
| Description: | The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design stages) allows organizations to influence the design of the system, system component, or system service. This early involvement in the system development life cycle helps organizations avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services or requiring system service providers to do so. Early identification of functions, ports, protocols, and services avoids costly retrofitting of controls after the system, component, or system service has been implemented. SA-9 describes the requirements for external system services. Organizations identify which functions, ports, protocols, and services are provided from external sources. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-4(10)  | TITLE: | ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS  |
| Description: | Products on the FIPS 201-approved products list meet NIST requirements for Personal Identity Verification (PIV) of Federal Employees and Contractors. PIV cards are used for multi-factor authentication in systems and organizations. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-5  | TITLE: | System Documentation  |
| Description: | System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-9  | TITLE: | External System Services  |
| Description: | External system services are provided by an external provider, and the organization has no direct control over the implementation of the required controls or the assessment of control effectiveness. Organizations establish relationships with external service providers in a variety of ways, including through business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, joint ventures, and supply chain exchanges. The responsibility for managing risks from the use of external system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a certain level of confidence that each provider in the consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust vary based on relationships between organizations and the external providers. Organizations document the basis for the trust relationships so that the relationships can be monitored. External system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define the expectations of performance for implemented controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-9(2)  | TITLE: | EXTERNAL SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES  |
| Description: | Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be useful when the need arises to understand the trade-offs involved in restricting certain functions and services or blocking certain ports and protocols. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-10  | TITLE: | Developer Configuration Management  |
| Description: | Organizations consider the quality and completeness of configuration management activities conducted by developers as direct evidence of applying effective security controls. Controls include protecting the master copies of material used to generate security-relevant portions of the system hardware, software, and firmware from unauthorized modification or destruction. Maintaining the integrity of changes to the system, system component, or system service requires strict configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. The configuration items that are placed under configuration management include the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the current running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and source code with previous versions; and test fixtures and documentation. Depending on the mission and business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance stage of the system development life cycle. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SA-11  | TITLE: | Developer Security Testing and Evaluation  |
| Description: | Developmental testing and evaluation confirms that the required controls are implemented correctly, operating as intended, enforcing the desired security and privacy policies, and meeting established security and privacy requirements. Security properties of systems and the privacy of individuals may be affected by the interconnection of system components or changes to those components. The interconnections or changes—including upgrading or replacing applications, operating systems, and firmware—may adversely affect previously implemented controls. Ongoing assessment during development allows for additional types of testing and evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as manual code review, security architecture review, and penetration testing, as well as and static analysis, dynamic analysis, binary analysis, or a hybrid of the three analysis approaches. Developers can use the analysis approaches, along with security instrumentation and fuzzing, in a variety of tools and in source code reviews. The security and privacy assessment plans include the specific activities that developers plan to carry out, including the types of analyses, testing, evaluation, and reviews of software and firmware components; the degree of rigor to be applied; the frequency of the ongoing testing and evaluation; and the types of artifacts produced during those processes. The depth of testing and evaluation refers to the rigor and level of detail associated with the assessment process. The coverage of testing and evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security and privacy assessment plans, flaw remediation processes, and the evidence that the plans and processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the system. Contracts may specify protection requirements for documentation. |
| Status: |  |

System and Communications Protection [SC] Family

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SC-1  | TITLE: | System and Communications Protection Policy and Procedures  |
| Description: | System and communications protection policy and procedures address the controls in the SC family that are implemented within systems and organizations. … |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SC-5  | TITLE: | Denial of Service Protection  |
| Description: | Denial-of-service events may occur due to a variety of internal and external causes, such as an attack by an adversary or a lack of planning to support organizational needs with respect to capacity and bandwidth. Such attacks can occur across a wide range of network protocols (e.g., IPv4, IPv6). A variety of technologies are available to limit or eliminate the origination and effects of denial-of-service events. For example, boundary protection devices can filter certain types of packets to protect system components on internal networks from being directly affected by or the source of denial-of-service attacks. Employing increased network capacity and bandwidth combined with service redundancy also reduces the susceptibility to denial-of-service events. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SC-7(3)  | TITLE: | BOUNDARY PROTECTION | ACCESS POINTS  |
| Description: | Limiting the number of external network connections facilitates monitoring of inbound and outbound communications traffic. The Trusted Internet Connection [DHS TIC] initiative is an example of a federal guideline that requires limits on the number of external network connections. Limiting the number of external network connections to the system is important during transition periods from older to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols). Such transitions may require implementing the older and newer technologies simultaneously during the transition period and thus increase the number of access points to the system. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SC-7(4)  | TITLE: | BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES  |
| Description: | External telecommunications services can provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol (BGP) routing, Domain Name System (DNS), and management protocols. See [SP 800-189] for additional information on the use of the resource public key infrastructure (RPKI) to protect BGP routes and detect unauthorized BGP announcements. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SC-20  | TITLE: | Secure Name /Address Resolution Service (Authoritative Source)  |
| Description: | Providing authoritative source information enables external clients, including remote Internet clients, to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. Systems that provide name and address resolution services include domain name system (DNS) servers. Additional artifacts include DNS Security Extensions (DNSSEC) digital signatures and cryptographic keys. Authoritative data includes DNS resource records. The means for indicating the security status of child zones include the use of delegation signer resource records in the DNS. Systems that use technologies other than the DNS to map between host and service names and network addresses provide other means to assure the authenticity and integrity of response data. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SC-21  | TITLE: | Secure Name /Address Resolution Service (Recursive or Caching Resolver)  |
| Description: | Each client of name resolution services either performs this validation on its own or has authenticated channels to trusted validation providers. Systems that provide name and address resolution services for local clients include recursive resolving or caching domain name system (DNS) servers. DNS client resolvers either perform validation of DNSSEC signatures, or clients use authenticated channels to recursive resolvers that perform such validations. Systems that use technologies other than the DNS to map between host and service names and network addresses provide some other means to enable clients to verify the authenticity and integrity of response data. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SC-22  | TITLE: | Architecture and Provisioning for Name/Address Resolution Service  |
| Description: | Systems that provide name and address resolution services include domain name system (DNS) servers. To eliminate single points of failure in systems and enhance redundancy, organizations employ at least two authoritative domain name system servers—one configured as the primary server and the other configured as the secondary server. Additionally, organizations typically deploy the servers in two geographically separated network subnetworks (i.e., not located in the same physical facility). For role separation, DNS servers with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients). DNS servers with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks, including the Internet). Organizations specify clients that can access authoritative DNS servers in certain roles (e.g., by address ranges and explicit lists). |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SC-39  | TITLE: | Process Isolation  |
| Description: | Systems can maintain separate execution domains for each executing process by assigning each process a separate address space. Each system process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process. Maintaining separate execution domains for executing processes can be achieved, for example, by implementing separate address spaces. Process isolation technologies, including sandboxing or virtualization, logically separate software and firmware from other software, firmware, and data. Process isolation helps limit the access of potentially untrusted software to other system resources. The capability to maintain separate execution domains is available in commercial operating systems that employ multi-state processor technologies. |
| Status: |  |

System and Information Integrity [SI] Family

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SI-1  | TITLE: | System and Information Integrity Policy and Procedures  |
| Description: | System and information integrity policy and procedures address the controls in the SI family that are implemented within systems and organizations. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SI-4(5)  | TITLE: | SYSTEM MONITORING | SYSTEM-GENERATED ALERTS  |
| Description: | Alerts may be generated from a variety of sources, including audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be automated and may be transmitted telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the alert notification list can include system administrators, mission or business owners, system owners, information owners/stewards, senior agency information security officers, senior agency officials for privacy, system security officers, or privacy officers. In contrast to alerts generated by the system, alerts generated by organizations in SI-4(12) focus on information sources external to the system, such as suspicious activity reports and reports on potential insider threats. |
| Status: |  |

|  |  |  |  |
| --- | --- | --- | --- |
| NFO Control: | SI-16  | TITLE: | Memory Protection  |
| Description: | Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Controls employed to protect memory include data execution prevention and address space layout randomization. Data execution prevention controls can either be hardware-enforced or software-enforced with hardware enforcement providing the greater strength of mechanism. |
| Status: |  |

1. System Interconnection Matrix

The following table identifies system interconnections with other in-scope system components. The table is meant to provide general interconnection information to protect the Organization’s Operational Security interests.

Table 8. System Interconnection Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| From System Component | To System Component | Purpose | Communication Method |
| Component Name | Component Name | Explain the purpose of the interconnection | Identify ports and protocols used |
|  |  |  |  |

1. Organization Information Security Responsibilities

The following table identifies which organizational role(s) is responsible for ensuring compliance with CMMC and NIST SP 800-171 Requirements.

Table 9. Information Security Responsibilities Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RQMNT | CMMC ID | CMMC TITLE | DESCRIPTION | RESPONSIBLE PARTY |
| 3.1.1  | AC.L2-3.1.1  | Authorized Access Control  | Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).  |  |
| 3.1.2  | AC.L2-3.1.2  | Transaction & Function Control  | Limit system access to the types of transactions and functions that authorized users are permitted to execute.  |  |
| 3.1.3  | AC.L2-3.1.3  | External Connections  | Control the flow of CUI in accordance with approved authorizations.  |  |
| 3.1.4  | AC.L2-3.1.4  | Control Public Information  | Separate the duties of individuals to reduce the risk of malevolent activity without collusion.  |  |
| 3.1.5  | AC.L2-3.1.5  | Control CUI Flow  | Employ the principle of least privilege, including for specific security functions and privileged accounts.  |  |
| 3.1.6  | AC.L2-3.1.6  | Separation of Duties  | Use non-privileged accounts or roles when accessing nonsecurity functions.  |  |
| 3.1.7  | AC.L2-3.1.7  | Least Privilege  | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.  |  |
| 3.1.8  | AC.L2-3.1.8  | Non-Privileged Account Use  | Limit unsuccessful logon attempts.  |  |
| 3.1.9  | AC.L2-3.1.9  | Privileged  Functions  | Provide privacy and security notices consistent with applicable CUI rules.  |  |
| 3.1.10  | AC.L2-3.1.10  | Unsuccessful Logan Attempts  | Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.  |  |
| 3.1.11  | AC.L2-3.1.11  | Privacy & Security Notices  | Terminate (automatically) a user session after a defined condition.  |  |
| 3.1.12  | AC.L2-3.1.12  | Session Lock  | Monitor and control remote access sessions.  |  |
| 3.1.13  | AC.L2-3.1.13  | Session Termination  | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.  |  |
| 3.1.14  | AC.L2-3.1.14  | Control Remote Access  | Route remote access via managed access control points.  |  |
| 3.1.15  | AC.L2-3.1.15  | Remote Access Confidentiality  | Authorize remote execution of privileged commands and remote access to security relevant information.  |  |
| 3.1.16  | AC.L2-3.1.16  | Remote Access Routing  | Authorize wireless access prior to allowing such connections.  |  |
| 3.1.17  | AC.L2-3.1.17  | Privileged  Remote Access  | Protect wireless access using authentication and encryption.  |  |
| 3.1.18  | AC.L2-3.1.18  | Wireless Access Authorization  | Control connection of mobile devices.  |  |
| 3.1.19  | AC.L2-3.1.19  | Wireless Access Protection  | Encrypt CUI on mobile devices and mobile computing platforms.  [Mobile devices and computing platforms include, for example, smartphones and tablets. 23  |  |
| 3.1.20  | AC.L2-3.1.20  | Mobile Device Connection  | Verify and control/limit connections to and use of external systems.  |  |
| 3.1.21  | AC.L2-3.1.21  | Encrypt CUI on  Mobile  | Limit use of portable storage devices on external systems.  |  |
| 3.1.22  | AC.L2-3.1.22  | Portable Storage Use  | Control CUI posted or processed on publicly accessible systems.  |  |
| 3.2.1  | AT.L2-3.2.1  | Role-Based Risk Awareness  | Ensure that managers, systems 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.  |  |
| 3.2.2  | AT.L2-3.2.2  | Role-Based Training  | Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.  |  |
| 3.2.3  | AT.L2-3.2.3  | Insider Threat Awareness  | Provide security awareness training on recognizing and reporting potential indicators of insider threat.  |  |
| 3.3.1  | AU.L2-3.3.1  | System Auditing  | 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.  |  |
| 3.3.2  | AU.L2-3.3.2  | User Accountability  | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.  |  |
| 3.3.3  | AU.L2-3.3.3  | Event Review  | Review and update logged events.  |  |
| 3.3.4  | AU.L2-3.3.4  | Audit Failure Alerting  | Alert in the event of an audit logging process failure.  |  |
| 3.3.5  | AU.L2-3.3.5  | Audit Correlation  | Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.  |  |
| 3.3.6  | AU.L2-3.3.6  | Reduction & Reporting  | Provide audit record reduction and report generation to support on-demand analysis and reporting.  |  |
| 3.3.7  | AU.L2-3.3.7  | Authoritative Time Source  | Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.  |  |
| 3.3.8  | AU.L2-3.3.8  | Audit Protection  | Protect audit information and audit logging tools from unauthorized access, modification, and deletion.  |  |
| 3.3.9  | AU.L2-3.3.9  | Audit Management  | Limit management of audit logging functionality to a subset of privileged users.  |  |
| 3.4.1  | CM.L2-3.4.1  | System Baselining  | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.  |  |
| 3.4.2  | CM.L2-3.4.2  | Security Configuration Enforcement  | Establish and enforce security configuration settings for information technology products employed in organizational systems.  |  |
| 3.4.3  | CM.L2-3.4.3  | System Change Management  | Track, review, approve or disapprove, and log changes to organizational systems.  |  |
| 3.4.4  | CM.L2-3.4.4  | Security Impact Analysis  | Analyze the security impact of changes prior to implementation.  |  |
| 3.4.5  | CM.L2-3.4.5  | Access Restrictions for Change  | Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.  |  |
| 3.4.6  | CM.L2-3.4.6  | Least Functionality  | Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.  |  |
| 3.4.7  | CM.L2-3.4.7  | Nonessential Functionality  | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.  |  |
| 3.4.8  | CM.L2-3.4.8  | Application Execution Policy  | 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.  |  |
| 3.4.9  | CM.L2-3.4.9  | User-Installed Software  | Control and monitor user-installed software.  |  |
| 3.5.1  | IA.L2-3.5.1  | Identification  | Identify system users, processes acting on behalf of users, and devices.  |  |
| 3.5.2  | IA.L2-3.5.2  | Authentication  | Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.  |  |
| 3.5.3  | IA.L2-3.5.3  | Multifactor Authentication  | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. 24 25  |  |
| 3.5.4  | IA.L2-3.5.4  | Replay-Resistant Authentication  | Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.  |  |
| 3.5.5  | IA.L2-3.5.5  | Identifier Reuse  | Prevent reuse of identifiers for a defined period.  |  |
| 3.5.6  | IA.L2-3.5.6  | Identifier Handling  | Disable identifiers after a defined period of inactivity.  |  |
| 3.5.7  | IA.L2-3.5.7  | Password Complexity  | Enforce a minimum password complexity and change of characters when new passwords are created.  |  |
| 3.5.8  | IA.L2-3.5.8  | Password Reuse  | Prohibit password reuse for a specified number of generations.  |  |
| 3.5.9  | IA.L2-3.5.9  | Temporary Passwords  | Allow temporary password use for system logons with an immediate change to a permanent password.  |  |
| 3.5.10  | IA.L2-3.5.10  | Cryptographically-Protected Passwords  | Store and transmit only cryptographically-protected passwords.  |  |
| 3.5.11  | IA.L2-3.5.11  | Obscure Feedback  | Obscure feedback of authentication information.  |  |
| 3.6.1  | IR.L2-3.6.1  | Incident Handling  | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.  |  |
| 3.6.2  | IR.L2-3.6.2  | Incident Reporting  | Track, document, and report incidents to designated officials and/or authorities both internal and external to Coalfire Federal.  |  |
| 3.6.3  | IR.L2-3.6.3  | Incident Response Testing  | Test the organizational incident response capability.  |  |
| 3.7.1  | MA.L2-3.7.1  | Perform Maintenance  | Perform maintenance on organizational systems.26  |  |
| 3.7.2  | MA.L2-3.7.2  | System Maintenance Control  | Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.  |  |
| 3.7.3  | MA.L2-3.7.3  | Equipment Sanitization  | Ensure equipment removed for off-site maintenance is sanitized of any CUI.  |  |
| 3.7.4  | MA.L2-3.7.4  | Media Inspection  | Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.  |  |
| 3.7.5  | MA.L2-3.7.5  | Nonlocal Maintenance  | Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.  |  |
| 3.7.6  | MA.L2-3.7.6  | Maintenance Personnel  | Supervise the maintenance activities of maintenance personnel without required access authorization.  |  |
| 3.8.1  | MP.L2-3.8.1  | Media Disposal  | Protect (i.e. physically control and securely store) system media containing CUI, both paper and digital.  |  |
| 3.8.2  | MP.L2-3.8.2  | Media Protection  | Limit access to CUI on system media to authorized users.  |  |
| 3.8.3  | MP.L2-3.8.3  | Media Access  | Sanitize or destroy system media containing CUI before disposal or release for reuse.  |  |
| 3.8.4  | MP.L2-3.8.4  | Media Markings  | Mark media with necessary CUI markings and distribution limitations.27  |  |
| 3.8.5  | MP.L2-3.8.5  | Media Accountability  | Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.  |  |
| 3.8.6  | MP.L2-3.8.6  | Portable Storage Encryption  | Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.  |  |
| 3.8.7  | MP.L2-3.8.7  | Removable Media  | Control the use of removable media on system components.  |  |
| 3.8.8  | MP.L2-3.8.8  | Shared Media  | Prohibit the use of portable storage devices when such devices have no identifiable owner.  |  |
| 3.8.9  | MP.L2-3.8.9  | Protect Backups  | Protect the confidentiality of backup CUI at storage locations.  |  |
| 3.9.1  | PS.L2-3.9.1  | Screen Individuals  | Screen individuals prior to authorizing access to organizational systems containing CUI.  |  |
| 3.9.2  | PS.L2-3.9.2  | Personnel Actions  | Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.  |  |
| 3.10.1  | PE.L2-3.10.1  | Limit Physical Access  | Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.  |  |
| 3.10.2  | PE.L2-3.10.2  | Escort Visitors  | Protect and monitor the physical facility and support infrastructure for organizational systems.  |  |
| 3.10.3  | PE.L2-3.10.3  | Physical Access Logs  | Escort visitors and monitor visitor activity.  |  |
| 3.10.4  | PE.L2-3.10.4  | Manage Physical Access  | Maintain audit logs of physical access.  |  |
| 3.10.5  | PE.L2-3.10.5  | Monitor Facility  | Control and manage physical access devices.  |  |
| 3.10.6  | PE.L2-3.10.6  | Alternative Work Sites  | Enforce safeguarding measures for CUI at alternate work sites.  |  |
| 3.11.1  | RA.L2-3.11.1  | Risk Assessments  | 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.  |  |
| 3.11.2  | RA.L2-3.11.2  | Vulnerability Scan  | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  |  |
| 3.11.3  | RA.L2-3.11.3  | Vulnerability Remediation  | Remediate vulnerabilities in accordance with risk assessments.  |  |
| 3.12.1  | CA.L2-3.12.1  | Security Control Assessment  | Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.  |  |
| 3.12.2  | CA.L2-3.12.2  | Plan of Action  | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.  |  |
| 3.12.3  | CA.L2-3.12.3  | Security Control Monitoring  | Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.  |  |
| 3.12.4  | CA.L2-3.12.4  | System Security Plan  | 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.28  |  |
| 3.13.1  | SC.L2-3.13.1  | Boundary Protection  | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.  |  |
| 3.13.2  | SC.L2-3.13.2  | Public-Access System Separation  | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.  |  |
| 3.13.3  | SC.L2-3.13.3  | Security Engineering  | Separate user functionality from system management functionality.  |  |
| 3.13.4  | SC.L2-3.13.4  | Role Separation  | Prevent unauthorized and unintended information transfer via shared system resources.  |  |
| 3.13.5  | SC.L2-3.13.5  | Shared Resource Control  | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.  |  |
| 3.13.6  | SC.L2-3.13.6  | Network Communication by Exception  | Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).  |  |
| 3.13.7  | SC.L2-3.13.7  | Split Tunneling  | 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).  |  |
| 3.13.8  | SC.L2-3.13.8  | Data in Transit  | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.  |  |
| 3.13.9  | SC.L2-3.13.9  | Connections Termination  | Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.  |  |
| 3.13.10  | SC.L2-3.13.10  | Key Management  | Establish and manage cryptographic keys for cryptography employed in organizational systems.  |  |
| 3.13.11  | SC.L2-3.13.11  | CUI Encryption  | Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.  |  |
| 3.13.12  | SC.L2-3.13.12  | Collaborative Device Control  | Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.29  |  |
| 3.13.13  | SC.L2-3.13.13  | Mobile Code  | Control and monitor the use of mobile code.  |  |
| 3.13.14  | SC.L2-3.13.14  | Voice over Internet Protocol  | Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.  |  |
| 3.13.15  | SC.L2-3.13.15  | Communications Authenticity  | Protect the authenticity of communications sessions.  |  |
| 3.13.16  | SC.L2-3.13.16  | Data at Rest  | Protect the confidentiality of CUI at rest.  |  |
| 3.14.1  | SI.L2-3.14.1  | Flaw Remediation  | Identify, report, and correct system flaws in a timely manner.  |  |
| 3.14.2  | SI.L2-3.14.2  | Malicious Code Protection  | Provide protection from malicious code at designated locations within organizational systems.  |  |
| 3.14.3  | SI.L2-3.14.3  | Update Malicious Code Protection  | Monitor system security alerts and advisories and take action in response.  |  |
| 3.14.4  | SI.L2-3.14.4  | System & File Scanning  | Update malicious code protection mechanisms when new releases are available.  |  |
| 3.14.5  | SI.L2-3.14.5  | Security Alerts & Advisories  | Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.  |  |
| 3.14.6  | SI.L2-3.14.6  | Monitor Communications for Attacks  | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.  |  |
| 3.14.7  | SI.L2-3.14.7  | Identify Unauthorized Use  | Identify unauthorized use of organizational systems.  |  |

1. Overall DFARS Clause 252.204-7012 Compliance

This table is provided to describe the organization’s compliance state to specific to DFARS Clause 252.204-7012.

Table 10. Overall DFARS Clause 252.204-7012 Compliance

|  |  |  |
| --- | --- | --- |
| Clause Paragraph | Requirement | Status |
| b)(2)(ii)(D) | External cloud service requirements |  |
| (c) | Cyber Incident Reporting Requirement |  |
| (d) | Malicious Software |  |
| (e) | Media Preservation and Protection |  |
| (f) | Access to Additional Information or Equipment Necessary |  |
| (g) | Cyber Incident Damage Assessment Activities |  |
| (h) | DoD Safeguarding/Use of Contractor Attributional/Proprietary Info |  |
| (m)(1) | Subcontracts: Flow down clause in subcontracts |  |
| (m)(1) | Subcontracts: CUI determination in subcontracts by Prime |  |
| (m)(2) | Subcontracts: Notification and incident report requirement |  |

1. Related Security Requirements

The following are Security Requirements related to this plan.

Table 11. Related Security Requirements

|  |  |  |
| --- | --- | --- |
| NISP SP 800-171 | CMMC ID | Description |
| 3.12.1 | CA.L2-3.12.1 | Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. |
| 3.12.2 | CA.L2-3.12.2 | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. |
| 3.12.4 | CA.L2-3.12.4 | 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. |

1. Ref NIST Special Publication 800-207, Zero Trust Architecture, para 2.1 [↑](#footnote-ref-2)