System Security Plan Template

Information System Name

Version

Instructions

This document is intended as a starting point for the IT System Security plan required by NIST 800-171 (3.12.4) and CMMC Level 3 (CA.2.157).

Each section includes a blue box of text like this which describes what the section is looking for and how to complete it. Once you have provided the information, you can remove this blue text.

This document has Confidential markings on it as the information provided once complete is considered confidential and should not be shared outside the organization, but the template itself can be shared.

Approved By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Approval Date: \_\_\_\_\_\_\_\_\_\_

*Insert Approver Title*

Approved By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Approval Date: \_\_\_\_\_\_\_\_\_\_

*Insert Approver Title*

Approved By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Approval Date: \_\_\_\_\_\_\_\_\_\_

*Insert Approver Title*

# Table of Contents

[Table of Contents 3](#_Toc81303872)

[1 Document Revision History 4](#_Toc81303873)

[2 Executive Summary 4](#_Toc81303874)

[3 System Identification 4](#_Toc81303875)

[4 System Operational Status 5](#_Toc81303876)

[Operational 5](#_Toc81303877)

[Under Development 5](#_Toc81303878)

[Major Modification 5](#_Toc81303879)

[5 General System Description 5](#_Toc81303880)

[6 System Environment 6](#_Toc81303881)

[7 System Interconnections/Information Sharing 6](#_Toc81303882)

[Data Flow 8](#_Toc81303883)

[Ports, Protocols, and Services 8](#_Toc81303884)

[8 Minimal Security Controls 8](#_Toc81303885)

[AC - Access Control 8](#_Toc81303886)

[AM – Asset Management 17](#_Toc81303887)

[AU - Audit and Accountability 18](#_Toc81303888)

[AT – Awareness and Training 23](#_Toc81303889)

[CM - Configuration Management 25](#_Toc81303890)

[IA - Identification and Authentication 29](#_Toc81303891)

[IR - Incident Response 34](#_Toc81303892)

[MA - Maintenance 38](#_Toc81303893)

[MP - Media Protection 41](#_Toc81303894)

[PS - Personnel Security 45](#_Toc81303895)

[PE - Physical Protection 47](#_Toc81303896)

[RE – Recovery 50](#_Toc81303897)

[RM - Risk Management 52](#_Toc81303898)

[CA - Security Assessment 56](#_Toc81303899)

[SA – Situational Awareness 59](#_Toc81303900)

[SC - System and Communications Protection 60](#_Toc81303901)

[SI - System and Information Integrity 68](#_Toc81303902)

[9 Template Revision History 73](#_Toc81303903)

# Document Revision History

This is not the Template’s revision history, but the System Security Plan’s revision history

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** |
|  |  |  |  |
|  |  |  |  |

# Executive Summary

Provide a brief summary of work being completed under the contract. Information to consider includes:

* An explanation of research or work being conducted
* An overview of outside organizations with which the contract is involved and how the organizations interact with each other. Examples of outside organizations might include:
* Field centers, clinical sites, clinical reading centers, and data collection centers
* Third party IT support vendors, etc.
* The roles and responsibilities of personnel as it relates to information collection, storage and sharing

# System Identification

*Identify the system name, type and owners. In the context of NIST 800-171, a* ***system*** *is a complete set of computers that support the function. For example, if you have a web service, the computer system that runs the web server and the computer system that runs the database is considered part of the same* ***system****.*

*Within this section consider including:*

* *Name of system(s)*
* *Whether it is a major application (ex. database/custom code) or general support system (ex. windows AD)*
* *System Information Type: Management and Support or Research focused*
* *A list of individuals who have administrative rights to workstations and servers*
* *Ownership contacts: Information Owner, Information Systems Owner*

|  |  |
| --- | --- |
| **Information System Owner** – the system owner of functional proponent/advocate for this system (usually the researcher) | |
| Name |  |
| Title |  |
| Department |  |
| Phone Number |  |
| Email |  |

|  |  |
| --- | --- |
| **Information System Management** (any IT staff assisting in the management of the system) | |
| Name |  |
| Title |  |
| Department |  |
| Phone Number |  |
| Email |  |

Copy and paste this table if more contacts are needed

# System Operational Status

*What is the current status of the system or parts of the system?*

*Operational – the system is in production*

*Under Development – the system is being designed, developed, or implemented*

*Undergoing a major modification – the system is undergoing a major conversion or transition*

*If the system is under development, outline the major activities and projected timeline to achieve operational status.*

## Operational

*Any parts of your system that are already operational*

## Under Development

*Any parts of the system that are still under development*

## Major Modification

*Any parts of the system that are undergoing a major modification*

# General System Description

*Provide a general description of the system. Outline what scope the system plays in conducting work for the overall contract. Detail the major functions of the information system and an overview of the system architecture including hardware and software components. For example, you could provide details on:*

*Significant use cases or user stories the system implements*

*Significant data or information inputs and outputs*

*Outline what types of data is collected and stored on the major system components and identify which business entity controls the data.*

# System Environment

*Include a system architecture diagram portraying all major functions within the system. Provide a detailed description of each major function. For example, description could include:*

* *Physical location*
* *Vendors for commercial software*
* *Groups/entities who have access to major functions*
* *Operating system*
* *Make and Model*
* *Licensed software for major functions*
* *Anti-Virus*
* *Firewalls*
* *DMZ*
* *Elements such as:*
  + *Web, Database and Application servers*
  + *E-mail services such as Microsoft Exchange Servers*
  + *Web-based applications and major application components such as web services or infrastructure products such as software frameworks*
  + *User Workstations and workstation software and specialized configurations*
  + *Scientific instruments and medical devices*
  + *Laboratory Information Systems*

*Be sure to identify the organization that hosts and manages each major function.*

# System Interconnections/Information Sharing

*Outline the major connections to the system, how information is shared, stored and backed up, and what types of information is transmitted. For example, detail any connections that occur through public facing web-applications, internal intranet connections and remote connections to the system. Outline the security measures that are in place to protect information such as remote VPN, HTTPS and user agreements.*

Table - System Interconnections

| **IP Address and Interface** | **External Organization Name and IP Address of System** | **External Point of Contact and Phone Number** | **Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)** | **Data Direction**  **(incoming, outgoing, or both)** | **Information Being Transmitted** | **Port Numbers** |
| --- | --- | --- | --- | --- | --- | --- |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |

## Data Flow

Describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. If necessary, include multiple data flow diagrams.

## Ports, Protocols, and Services

These are the ports protocols and services running on this system.

Table - Ports, Protocols and Services

| **Ports (TCP/UDP)** | **Protocol(s)** | **Services** | **Purpose** | **Used By** |
| --- | --- | --- | --- | --- |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |

# Minimal Security Controls

These are the minimum required security controls to meet CMMC Level 3.

AC - Access Control

AC.1.001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

| AC.1.001 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute

| AC.1.002 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.1.003 Verify and control/limit connections to and use of external information systems

| AC.1.003 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.1.004 Control information posted or processed on publicly accessible systems

| AC.1.004 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.005 Provide privacy and security notices consistent with applicable CUI rules

| AC.2.005 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.006 Limit use of portable storage devices on external systems

| AC.2.006 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.007 Employ the principle of least privilege, including for specific security functions and privileged accounts

| AC.2.007 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.008 Use non-privileged accounts or roles when accessing nonsecurity functions

| AC.2.008 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.009 Limit unsuccessful logon attempts

| AC.2.009 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.010 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity

| AC.2.010 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.011 Authorize wireless access prior to allowing such connections

| AC.2.011 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.013 Monitor and control remote access sessions

| AC.2.013 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.015 Route remote access via managed access control points

| AC.2.015 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.998 Document the CMMC Practices to implement the Access Control policy

| AC.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.2.999 Establish a policy that includes Access Control

| AC.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.3.012 Protect wireless access using authentication and encryption

| AC.3.012 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.3.014 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions

| AC.3.014 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.3.017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion

| AC.3.017 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.3.018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs

| AC.3.018 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.3.019 Terminate (automatically) user sessions after a defined condition

| AC.3.019 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.3.020 Control connection of mobile devices

| AC.3.020 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.3.021 Authorize remote execution of privileged commands and remote access to security-relevant information.

| AC.3.021 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.3.022 Encrypt CUI on mobile devices and mobile computing platforms

| AC.3.022 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AC.3.997 Establish, maintain, and resource a plan that includes Access Control

| AC.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AM – Asset Management

AM.2.998 Document the CMMC Practices to implement the Asset Management policy

| AM.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AM.2.999 Establish a policy that includes Asset Management

| AM.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AM.3.036 Define procedures for the handling of CUI data

| AU.2.041 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AM.3.997 Establish, maintain, and resource a plan that includes Asset Management

| AM.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU - Audit and Accountability

AU.2.041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions

| AU.2.041 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.2.042 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

| AU.2.042 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.2.043 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records

| AU.2.043 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.2.044 Review audit logs

| AU.2.044 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.2.998 Document the CMMC Practices to implement the Audit and Accountability policy

| AU.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.2.999 Establish a policy that includes Audit and Accountability

| AU.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.3.045 Review and update logged events

| AU.3.045 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.3.046 Alert in the event of an audit logging process failure

| AU.3.046 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.3.048 Collet audit information (e.g., logs) into one or more central repositories

| AU.3.048 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.3.049 Protect audit information and audit logging tools from unauthorized access, modification, and deletion

| AU.3.049 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.3.050 Limit management of audit logging functionality to a subset of privileged users

| AU.3.050 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.3.051 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity

| AU.3.051 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.3.052 Provide audit record reduction and report generation to support on-demand analysis and reporting

| AU.3.052 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AU.3.997 Establish, maintain, and resource a plan that includes Audit and Accountability

| AU.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AT – Awareness and Training

AT.2.056 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

| AT.2.056 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AT.2.057 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities

| AT.2.057 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AT.2.998 Document the CMMC Practices to implement the Awareness and Training policy

| AT.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AT.2.999 Establish a policy that includes Awareness and Training

| AT.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AT.3.058 Provide security awareness training on recognizing and reporting potential indicators of insider threat

| AT.3.058 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

AT.3.997 Establish, maintain, and resource a plan that includes Awareness and Training

| AT.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM - Configuration Management

CM.2.061 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles

| CM.2.061 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.2.062 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities

| CM.2.062 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.2.063 Control and monitor user-installed software

| CM.2.063 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.2.064 Establish and enforce security configuration settings for information technology products employed in organizational systems

| CM.2.064 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.2.065 Track, review, approve, or disapprove, and log changes to organizational systems

| CM.2.065 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.2.066 Analyze the security impact of changes prior to implementation

| CM.2.066 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.2.998 Document the CMMC Practices to implement the Configuration Management policy

| CM.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.2.999 Establish a policy that includes Configuration Management

| CM.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.3.067 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems

| CM.3.067 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.3.068 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services

| CM.3.068 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.3.069 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software

| CM.3.069 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CM.3.997 Establish, maintain, and resource a plan that includes Configuration Management

| CM.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA - Identification and Authentication

IA.1.076 Identify information system users, processes acting on behalf of users, or devices

| IA.1.076 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.1.077 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems

| IA.1.077 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.2.078 Enforce a minimum password complexity and change of characters when new passwords are created

| IA.2.078 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.2.079 Prohibit password reuse for a specified number of generations

| IA.2.079 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.2.080 Allow temporary password use for system logons with an immediate change to a permanent password

| IA.2.080 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.2.081 Store and transmit only cryptographically-protected passwords

| IA.2.081 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.2.082 Obscure feedback of authentication information

| IA.2.082 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.2.998 Document the CMMC Practices to implement the Identification and Authentication policy

| IA.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.2.999 Establish a policy that includes Identification and Authentication

| IA.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.3.083 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

| IA.3.038 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.3.084 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts

| IA.3.084 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.3.085 Prevent the reuse of identifiers for a defined period

| IA.3.085 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.3.086 Disable identifiers after a defined period of inactivity

| IA.3.086 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IA.3.997 Establish, maintain, and resource a plan that includes Identification and Authentication

| IA.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IR - Incident Response

IR.2.092 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities

| IR.2.092 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IR.2.093 Detect and report events

| IR.2.093 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IR.2.094 Analyze and triage events to support event resolution and incident declaration

| IR.2.094 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IR.2.096 Develop and implement responses to declared incidents according to pre-defined procedures

| IR.2.096 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IR.2.097 Perform root cause analysis on incidents to determine underlying causes

| IR.2.097 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IR.2.998 Document the CMMC Practices to implement the Incident Response policy

| IR.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IR.2.999 Establish a policy that includes Incident Response

| IR.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IR.3.098 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization

| IR.3.098 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IR.3.099 Test the organizational incident response capability

| IR.3.099 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

IR.3.997 Establish, maintain, and resource a plan that includes Incident Response

| IR.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MA - Maintenance

MA.2.111 Perform maintenance on organizational systems

| MA.2.111 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MA.2.112 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance

| MA.2.112 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MA.2.113 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete

| MA.2.113 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MA.2.114 Supervise the maintenance activities of personnel without required access authorization.

| MA.2.114 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MA.2.998 Document the CMMC Practices to implement the Maintenance policy

| MA.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MA.2.999 Establish a policy that includes Maintenance

| MA.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MA.3.115 Ensure equipment removed for off-site maintenance is sanitized of any CUI

| MA.3.115 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MA.3.116 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems

| MA.3.116 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MA.3.997 Establish, maintain, and resource a plan that includes Maintenance

| MA.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP - Media Protection

MP.1.118 Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse

| MP.1.118 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP.2.119 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital

| MP.2.119 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP.2.120 Limit access to CUI on system media to authorized users

| MP.2.120 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP.2.121 Control the use of removable media on system components

| MP.2.121 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP.2.998 Document the CMMC Practices to implement the Media Protection policy

| MP.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP.2.999 Establish a policy that includes Media Protection

| MP.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP.3.122 Mark media with necessary CUI markings and distribution limitations

| MP.3.122 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP.3.123 Prohibit the use of portable storage devices when such devices have no identifiable owner

| MP.3.123 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP.3.124 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas

| MP.3.124 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP.3.125 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards

| MP.3.125 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

MP.3.997 Establish, maintain, and resource a plan that includes Media Protection

| MP.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PS - Personnel Security

PS.2.127 Screen individuals prior to authorizing access to organizational systems containing CUI

| PS.2.127 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PS.2.128 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers

| PS.2.128 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PS.2.998 Document the CMMC Practices to implement the Personnel Security policy

| PS.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PS.2.999 Establish a policy that includes Personnel Security

| PS.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PS.3.997 Establish, maintain, and resource a plan that includes Personnel Security

| PS.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PE - Physical Protection

PE.1.131 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals

| PE.1.131 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PE.1.132 Escort visitors and monitor visitor activity

| PE.1.132 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PE.1.133 Maintain audit logs of physical access

| PE.1.133 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PE.1.134 Control and manage physical access devices

| PE.1.134 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PE.2.135 Protect and monitor the physical facility and support infrastructure for organizational systems

| PE.2.135 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PE.2.998 Document the CMMC Practices to implement the Physical Protection policy

| PE.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PE.2.999 Establish a policy that includes Physical Protection

| PE.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PE.3.136 Enforce safeguarding measures for CUI at alternate work sites.

| PE.3.136 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

PE.3.997 Establish, maintain, and resource a plan that includes Physical Protection

| PE.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RE – Recovery

RE.2.137 Regularly perform and test data back-ups

| RE.2.137 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RE.2.138 Protect the confidentiality of backup CUI at storage locations

| RE.2.138 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RE.2.998 Document the CMMC Practices to implement the Recovery policy

| RE.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RE.2.999 Establish a policy that includes Recovery

| RE.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RE.3.139 Regularly perform complete, comprehensive, and resilient data back-ups as organizational defined.

| RE.3.139 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RE.3.997 Establish, maintain, and resource a plan that includes Recovery

| RE.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RM - Risk Management

RM.2.141 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

| RM.2.141 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RM.2.142 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified

| RM.2.142 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RM.2.143 Remediate vulnerabilities in accordance with risk assessments.

| RM.2.143 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RM.2.998 Document the CMMC Practices to implement the Risk Management policy

| RM.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RM.2.999 Establish a policy that includes Risk Management

| RM.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RM.3.144 Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria

| RM.3.144 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RM.3.146 Develop and implement risk mitigation plans

| RM.3.146 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RM.3.147 Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk

| RM.3.147 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

RM.3.997 Establish, maintain, and resource a plan that includes Risk Management

| RM.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CA - Security Assessment

CA.2.157 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.

| CA.2.157 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CA.2.158 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application

| 3.12.1 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CA.2.159 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems

| CA.2.159 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CA.2.998 Document the CMMC Practices to implement the Security Assessment policy

| CA.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CA.2.999 Establish a policy that includes Security Assessment

| CA.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CA.3.161 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls

| CA.3.161 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CA.3.162 Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk

| CA.3.162 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

CA.3.997 Establish, maintain, and resource a plan that includes Security Assessment

| CA.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SA – Situational Awareness

SA.2.998 Document the CMMC Practices to implement the Situational Awareness policy

| SA.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SA.2.999 Establish a policy that includes Situational Awareness

| SA.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SA.3.169 Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders

| SA.3.169 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SA.3.997 Establish, maintain, and resource a plan that includes Situational Awareness

| SA.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC - System and Communications Protection

SC.1.175 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems

| SC.1.175 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.1.176 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks

| SC.1.176 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.2.178 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device

| SC.2.178 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.2.179 Use encrypted sessions for the management of network devices

| SC.2.179 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.2.998 Document the CMMC Practices to implement the System and Communications Protection policy

| SC.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.2.999 Establish a policy that includes System and Communications Protection

| SC.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.177 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI

| SC.3.177 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.180 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems

| SC.3.180 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.181 Separate user functionality from system management functionality

| SC.3.181 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.182 Prevent unauthorized and unintended information transfer via shared system resources

| SC.3.182 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.183 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception)

| SC.3.183 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.184 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling)

| SC.3.184 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.185 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards

| SC.3.185 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.186 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity

| SC.3.186 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.187 Establish and manage cryptographic keys for cryptography employed in organizational systems

| SC.3.187 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.188 Control and monitor the use of mobile code

| SC.3.188 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.189 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

| SC.3.189 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.190 Protect the authenticity of communications sessions

| SC.3.190 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.191 Protect the confidentiality of CUI at rest

| SC.3.191 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.192 Implement Domain Name System (DNS) filtering services

| SC.3.192 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.193 Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter)

| SC.3.193 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SC.3.997 Establish, maintain, and resource a plan that includes System and Communications Protection

| SC.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI - System and Information Integrity

SI.1.210 Identify, report, and correct information and information system flaws in a timely manner

| SI.1.210 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.1.211 Provide protection from malicious code at appropriate locations within organizational information systems

| SI.1.211 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.1.212 Update malicious code protection mechanisms when new releases are available

| SI.1.212 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.1.213 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

| SI.1.213 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.2.214 Monitor system security alerts and advisories and take action in response

| SI.2.214 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.2.216 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks

| SI.2.216 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.2.217 Identify unauthorized use of organizational systems.

| SI.2.217 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.2.998 Document the CMMC Practices to implement the System and Information Integrity policy

| SI.2.998 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.2.999 Establish a policy that includes System and Information Integrity

| SI.2.999 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.3.218 Employ spam protection mechanisms at information system access entry and exit points

| SI.3.218 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.3.219 Implement email forgery protections

| SI.3.219 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.3.220 Utilize sandboxing to detect or block potentially malicious email

| SI.3.220 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

SI.3.997 Establish, maintain, and resource a plan that includes System and Information Integrity

| SI.3.997 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

# Template Revision History

This is the revision history of this template. This section can be removed once you’ve completed your document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** |
| 1.0 | 31-AUG-2021 | Lbowser <Laura Raderman> | Initial Document |
|  |  |  |  |