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).

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.

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

*Insert Approver Title*

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

*Insert Approver Title*

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

*Insert Approver Title*

# Table of Contents

[1 Document Revision History 4](#_Toc492902529)

[2 Executive Summary 4](#_Toc492902530)

[3 System Identification 4](#_Toc492902531)

[4 System Operational Status 5](#_Toc492902532)

[Operational 5](#_Toc492902533)

[5 General System Description 5](#_Toc492902534)

[6 System Environment 6](#_Toc492902535)

[Computing Services Campus Cloud Environment 6](#_Toc492902536)

[7 System Interconnections/Information Sharing 6](#_Toc492902537)

[Data Flow 8](#_Toc492902538)

[Ports, Protocols, and Services 8](#_Toc492902539)

[8 Minimal Security Controls 8](#_Toc492902540)

[3.1 Access Control 9](#_Toc492902541)

[9 Control Implementation Summary 14](#_Toc492902542)

[10 Template Revision History 15](#_Toc492902543)

# 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 NIST 800-171. The control numbering below is consistent with NIST SP 800-171.

* + 1. Access Control
       1. Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).

| 3.1.1 | 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? | |

* + - 1. Limit system access to the types of transactions and functions that authorized users are permitted to execute

| 3.1.2 | 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? | |

* + - 1. Control the flow of CUI in accordance with approved authorizations

| 3.1.3 | 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? | |

* + - 1. Separate the duties of individuals to reduce the risk of malevolent activity without collusion

| 3.1.4 | 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? | |

* + - 1. Employ the principle of least privilege, including for specific security functions and privileged accounts

| 3.1.5 | 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? | |

* + - 1. Use non-privileged accounts or roles when accessing non-security functions

| 3.1.6 | 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? | |

* + - 1. Prevent non-privileged users from executing privileged functions and audit the execution of such functions

| 3.1.7 | 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? | |

* + - 1. Limit unsuccessful logon attempts

| 3.1.8 | 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? | |

* + - 1. Provide privacy and security notices consistent with applicable CUI rules

| 3.1.9 | 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? | |

* + - 1. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity

| 3.1.10 | 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? | |

* + - 1. Terminate (automatically) a user session after a defined condition

| 3.1.11 | 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? | |

* + - 1. Monitor and control remote access sessions

| 3.1.12 | 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? | |

* + - 1. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions

| 3.1.13 | 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? | |

* + - 1. Route remote access via managed access control points

| 3.1.14 | 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? | |

* + - 1. Authorize remote execution of privileged commands and remote access to security-relevant information.

| 3.1.15 | 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? | |

* + - 1. Authorize wireless access prior to allowing such connections

| 3.1.16 | 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? | |

* + - 1. Protect wireless access using authentication and encryption

| 3.1.17 | 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? | |

* + - 1. Control connection of mobile devices

| 3.1.18 | 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? | |

* + - 1. Encrypt CUI on mobile devices and mobile computing platforms

| 3.1.19 | 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? | |

* + - 1. Verify and control/limit connections to and use of external systems

| 3.1.20 | 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? | |

* + - 1. Limit use of organizational portable storage devices on external systems

| 3.1.21 | 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? | |

* + - 1. Control CUI posted or processed on publicly accessible systems

| 3.1.22 | 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? | |

* + 1. Awareness and Training
       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

| 3.2.1 | 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? | |

* + - 1. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities

| 3.2.2 | 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? | |

* + - 1. Provide security awareness training on recognizing and reporting potential indicators of insider threat

| 3.2.3 | 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? | |

* + 1. Audit and Accountability
       1. Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity

| 3.3.1 | 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? | |

* + - 1. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions

| 3.3.2 | 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? | |

* + - 1. Review and update audited events

| 3.3.3 | 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? | |

* + - 1. Alert in the event of an audit process failure

| 3.3.4 | 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? | |

* + - 1. Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity

| 3.3.5 | 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? | |

* + - 1. Provide audit reduction and report generation to support on-demand analysis and reporting

| 3.3.6 | 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? | |

* + - 1. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records

| 3.3.7 | 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? | |

* + - 1. Protect audit information and audit tools from unauthorized access, modification, and deletion

| 3.3.8 | 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? | |

* + - 1. Limit management of audit functionality to a subset of privileged users

| 3.3.9 | 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? | |

* + 1. Configuration Management
       1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles

| 3.4.1 | 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? | |

* + - 1. Establish and enforce security configuration settings for information technology products employed in organizational systems

| 3.4.2 | 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? | |

* + - 1. Track, review, approve/disapprove, and audit changes to organizational systems

| 3.4.3 | 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? | |

* + - 1. Analyze the security impact of changes prior to implementation

| 3.4.4 | 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? | |

* + - 1. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems

| 3.4.5 | 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? | |

* + - 1. Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities

| 3.4.6 | 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? | |

* + - 1. Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services

| 3.4.7 | 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? | |

* + - 1. Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or denyall, permit-by-exception (whitelisting) policy to allow the execution of authorized software

| 3.4.8 | 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? | |

* + - 1. Control and monitor user-installed software

| 3.4.9 | 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? | |

* + 1. Identification and Authentication
       1. Identify system users, processes acting on behalf of users, or devices

| 3.5.1 | 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? | |

* + - 1. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems

| 3.5.2 | 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? | |

* + - 1. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts

| 3.5.3 | 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? | |

* + - 1. Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts

| 3.5.4 | 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? | |

* + - 1. Prevent reuse of identifiers for a defined period

| 3.5.5 | 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? | |

* + - 1. Disable identifiers after a defined period of inactivity

| 3.5.6 | 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? | |

* + - 1. Enforce a minimum password complexity and change of characters when new passwords are created

| 3.5.7 | 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? | |

* + - 1. Prohibit password reuse for a specified number of generations

| 3.5.8 | 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? | |

* + - 1. Allow temporary password use for system logons with an immediate change to a permanent password

| 3.5.9 | 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? | |

* + - 1. Store and transmit only cryptographically-protected passwords

| 3.5.10 | 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? | |

* + - 1. Obscure feedback of authentication information

| 3.5.11 | 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? | |

* + 1. Incident Response
       1. Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities

| 3.6.1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Security Office | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

* + - 1. Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization

| 3.6.2 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Security Office | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

* + - 1. Test the organizational incident response capability

| 3.6.3 | Control Summary Information |
| --- | --- |
| Responsible Role: Information Security Office | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| What is the solution and how is it implemented? | |

* + 1. Maintenance
       1. Perform maintenance on organizational systems

| 3.7.1 | 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? | |

* + - 1. Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance

| 3.7.2 | 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? | |

* + - 1. Ensure equipment removed for off-site maintenance is sanitized of any CUI

| 3.7.3 | 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? | |

* + - 1. Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems

| 3.7.4 | 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? | |

* + - 1. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete

| 3.7.5 | 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? | |

* + - 1. Supervise the maintenance activities of maintenance personnel without required access authorization.

| 3.7.6 | 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? | |

* + 1. Media Protection
       1. Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital

| 3.8.1 | 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? | |

* + - 1. Limit access to CUI on system media to authorized users

| 3.8.2 | 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? | |

* + - 1. Sanitize or destroy system media containing CUI before disposal or release for reuse

| 3.8.3 | 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? | |

* + - 1. Mark media with necessary CUI markings and distribution limitations

| 3.8.4 | 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? | |

* + - 1. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas

| 3.8.5 | 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? | |

* + - 1. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards

| 3.8.6 | 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? | |

* + - 1. Control the use of removable media on system components

| 3.8.7 | 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? | |

* + - 1. Prohibit the use of portable storage devices when such devices have no identifiable owner

| 3.8.8 | 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? | |

* + - 1. Protect the confidentiality of backup CUI at storage locations.

| 3.8.9 | 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? | |

* + 1. Personnel Security
       1. Screen individuals prior to authorizing access to organizational systems containing CUI

| 3.9.1 | 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? | |

* + - 1. Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers

| 3.9.2 | 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? | |

* + 1. Physical Protection
       1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals

| 3.10.1 | 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? | |

* + - 1. Protect and monitor the physical facility and support infrastructure for organizational systems

| 3.10.2 | 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? | |

* + - 1. Escort visitors and monitor visitor activity

| 3.10.3 | 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? | |

* + - 1. Maintain audit logs of physical access

| 3.10.4 | 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? | |

* + - 1. Control and manage physical access devices

| 3.10.5 | 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? | |

* + - 1. Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

| 3.10.6 | 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? | |

* + 1. Risk Assessment
       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

| 3.11.1 | 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? | |

* + - 1. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified

| 3.11.2 | 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? | |

* + - 1. Remediate vulnerabilities in accordance with assessments of risk.

| 3.11.3 | 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? | |

* + 1. Security Assessment
       1. 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? | |

* + - 1. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems

| 3.12.2 | 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? | |

* + - 1. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls

| 3.12.3 | 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? | |

* + - 1. 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.

| 3.12.4 | 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? | |

* + 1. System and Communications Protection
       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

| 3.13.1 | 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? | |

* + - 1. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems

| 3.13.2 | 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? | |

* + - 1. Separate user functionality from system management functionality

| 3.13.3 | 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? | |

* + - 1. Prevent unauthorized and unintended information transfer via shared system resources

| 3.13.4 | 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? | |

* + - 1. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks

| 3.13.5 | 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? | |

* + - 1. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception

| 3.13.6 | 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? | |

* + - 1. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks

| 3.13.7 | 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? | |

* + - 1. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards

| 3.13.8 | 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? | |

* + - 1. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity

| 3.13.9 | 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? | |

* + - 1. Establish and manage cryptographic keys for cryptography employed in organizational systems

| 3.13.10 | 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? | |

* + - 1. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI

| 3.13.11 | 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? | |

* + - 1. Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device

| 3.13.12 | 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? | |

* + - 1. Control and monitor the use of mobile code

| 3.13.13 | 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? | |

* + - 1. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

| 3.13.14 | 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? | |

* + - 1. Protect the authenticity of communications sessions

| 3.13.15 | 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? | |

* + - 1. Protect the confidentiality of CUI at rest

| 3.13.16 | 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? | |

* + 1. System and Information Integrity
       1. Identify, report, and correct information and system flaws in a timely manner

| 3.14.1 | 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? | |

* + - 1. Provide protection from malicious code at appropriate locations within organizational systems

| 3.14.2 | 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? | |

* + - 1. Monitor system security alerts and advisories and take appropriate actions in response

| 3.14.3 | 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? | |

* + - 1. Update malicious code protection mechanisms when new releases are available

| 3.14.4 | 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? | |

* + - 1. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

| 3.14.5 | 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? | |

* + - 1. Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks

| 3.14.6 | 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? | |

* + - 1. Identify unauthorized use of organizational systems.

| 3.14.7 | 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 | 25-SEP-2017 | Lbowser <Laura Raderman> | Initial Document |
|  |  |  |  |