**System Security Plan**

WSU SSP for [Information System Name]

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

Data Categorization Information
Creation Date: November 4, 2021
WSU Data Classification: **NON-PUBLIC**

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Description | Author |
| 1.0 |  | Initial Release |  |
|  |  |  |  |
|   |  |

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.

Contents

[Revision History ii](#_Toc99020975)

[1. Executive Summary 1](#_Toc99020976)

[2. System Identification 1](#_Toc99020977)

[3. System Operational Status 2](#_Toc99020978)

[3.1. Operational 2](#_Toc99020979)

[3.2. Under Development 2](#_Toc99020980)

[3.3. Major Modification 2](#_Toc99020981)

[4. General System Description 3](#_Toc99020982)

[4.1. Related Laws/Regulations/Policies 3](#_Toc99020983)

[5. System Environment 3](#_Toc99020984)

[6. System Interconnections/Information Sharing 4](#_Toc99020985)

[6.1. Data Flow 1](#_Toc99020986)

[6.2. Ports, Protocols, and Services 1](#_Toc99020987)

[7. Security Controls 1](#_Toc99020988)

[8. Effective Dates 2](#_Toc99020989)

[9. Review Cycle 2](#_Toc99020990)

[Appendix A: Glossary 3](#_Toc99020991)

 [3](#_Toc99020992)

[Appendix B: 4](#_Toc99020993)

# Executive Summary

|  |
| --- |
| **Information Owner** – See WSU BPPM 87.01 for definition of Information Owner |
| Name |  |
| Title |  |
| Business Unit |  |
| Phone Number |  |
| Email |  |

Provide a brief summary of work being completed by the information system. Information to consider includes:

* An explanation of research or work being conducted
* An overview of outside organizations with which a system/service/contract is involved and how the organizations interact with each other. Examples of outside organizations might include: external Business Units, field centers, clinical sites, clinical reading centers, and data collection centers or 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** – See WSU BPPM 87.01 for definition of Data Custodian |
| Name |  |
| Title |  |
| Department |  |
| Phone Number |  |
| Email |  |

|  |
| --- |
| **Information System Data Custodian** – See WSU BPPM 87.01 for definition of Data Custodian |
| Name |  |
| Title |  |
| Department |  |
| Phone Number |  |
| Email |  |

# 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.*

*Using the data definitions in* ***Executive Policy (EP) 8****, provide the classification of the data.*

## Related Laws/Regulations/Policies

*List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.*

# 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 2 - 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** |
| --- | --- | --- | --- | --- | --- | --- |
| <IP Address/Interface> | <External Org/IP> | <External Org POC><Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <IP Address/Interface> | <External Org/IP> | <External Org POC><Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <IP Address/Interface> | <External Org/IP> | <External Org POC><Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <IP Address/Interface> | <External Org/IP> | <External Org POC><Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <IP Address/Interface> | <External Org/IP> | <External Org POC><Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <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

*List the ports protocols and services running on this system.*

Table 2 - 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> |

# Security Controls

*Complete and attach Appendix B –* ***WSU NIST 171 Compliance & Risk Template****.*

*The NIST 800-171 Compliance Template tab provides the list of required NIST 171 information security controls. Using the NIST Handbook tab on the Compliance Template, please complete column E, Assigned Stakeholder, and Column F, Implemented Safeguards on the system.*

# Effective Dates

The effective date is to be identified in this section.

# Review Cycle

System Security Plans are to be reviewed and updated at least annually or whenever significant changes made to the system.

# Appendix A: Glossary

|  |  |
| --- | --- |
| Term | Definition |
| Information system | A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. |

# Appendix B:

***NIST SP 800-171 Compliance & Risk Template for WSU Owned Systems and Services***