[Insert Logo]

{{SSP|SECURITYPLAN.CSPADDRESS}}

{{SSP|SECURITYPLAN.CSPOFFICE}}

{{SSP|SECURITYPLAN.CSPCITYSTATE}}

**System Security Plan for the {{SSP|SECURITYPLAN.SYSTEMNAME}}**

{{SSP|SECURITYPLAN.VERSION}}

{{SSP|SECURITYPLAN.DATESUBMITTED}}

Table of Contents

[1. SYSTEM IDENTIFICATION 4](#_Toc130922763)

[System Name/Title 4](#_Toc130922764)

[System Unique Identifier 4](#_Toc130922765)

[System Categorization 4](#_Toc130922766)

[Responsible Organization 4](#_Toc130922767)

[Information System Owner 4](#_Toc130922768)

[Authorizing Official 4](#_Toc130922769)

[Information System Security Officer 5](#_Toc130922770)

[Information System Operational Status 5](#_Toc130922771)

[Information System Type 5](#_Toc130922772)

[General Description and Purpose 5](#_Toc130922773)

[Authorization Boundary 5](#_Toc130922774)

[User Roles 5](#_Toc130922775)

[Information Types 6](#_Toc130922776)

[2. SYSTEM ENVIRONMENT 6](#_Toc130922777)

[Hardware Inventory 6](#_Toc130922778)

[Software Inventory 6](#_Toc130922779)

[System Interconnections/Information Sharing 6](#_Toc130922780)

[Data Flow 6](#_Toc130922781)

[Ports, Protocols and Services 7](#_Toc130922782)

[3. MINIMUM SECURITY CONTROLS 7](#_Toc130922783)

[Access Control (AC) 7](#_Toc130922784)

[Awareness and Training (AT) 7](#_Toc130922785)

[Audit and Accountability (AU): 8](#_Toc130922786)

[Assessment, Authorization, and Monitoring (CA) 8](#_Toc130922787)

[Configuration Management (CM) 8](#_Toc130922788)

[Contingency Planning (CP) 9](#_Toc130922789)

[Identification and Authentication (IA) 9](#_Toc130922790)

[Incident Response (IR) 9](#_Toc130922791)

[Maintenance (MA) 10](#_Toc130922792)

[Media Protection (MP) 10](#_Toc130922793)

[Physical and Environmental Protection (PE) 10](#_Toc130922794)

[Planning (PL) 11](#_Toc130922795)

[Program Management (PM) 11](#_Toc130922796)

[Personnel Security (PS) 12](#_Toc130922797)

[PII Processing and Transparency (PT) 12](#_Toc130922798)

[Risk Assessment (RA) 12](#_Toc130922799)

[System and Services Acquisition (SA) 13](#_Toc130922800)

[System and Communications Protection (SC) 13](#_Toc130922801)

[System and Information Integrity (SI) 13](#_Toc130922802)

[Supply Chain Risk Management (SR) 14](#_Toc130922803)

[4. SYSTEM SECURITY PLAN APPROVAL 14](#_Toc130922804)

[System Security Plan Completion Date 14](#_Toc130922805)

[System Security Plan Approval Date 14](#_Toc130922806)

[5. RECORD OF CHANGES 15](#_Toc130922807)

# SYSTEM IDENTIFICATION

## System Name/Title

{{SSP|SECURITYPLAN.SYSTEMNAME}}

## System Unique Identifier

{{SSP|SECURITYPLAN.OTHERIDENTIFIER}}

## System Categorization

{{SSP|SECURITYPLAN.OVERALLCATEGORIZATION}}

## Categorization Justification

{{SSP|SECURITYPLAN.CATEGORIZATIONJUSTIFICATION}}

## Responsible Organization

|  |  |
| --- | --- |
| Name: | {{SSP|SECURITYPLAN.CSPORGNAME}} |
| Address: | {{SSP|SECURITYPLAN.CSPADDRESS}}  {{SSP|SECURITYPLAN.CSPOFFICE}}  {{SSP|SECURITYPLAN.CSPCITYSTATE}} |
| Phone: |  |

## Information System Owner

**Point of contact that owns the system:**

|  |  |
| --- | --- |
| Name: | {{SSP|SECURITYPLAN.SYSTEMOWNER.FULLNAME}} |
| Title: | {{SSP|SECURITYPLAN.SYSTEMOWNER.JOBTITLE}} |
| Office Address: | {{SSP|SECURITYPLAN.SYSTEMOWNER.COMPANY}}  {{SSP|SECURITYPLAN.SYSTEMOWNER.ADDRESS}} |
| Work Phone: | {{SSP|SECURITYPLAN.SYSTEMOWNER.WORKPHONE}} |
| e-Mail Address: | {{SSP|SECURITYPLAN.SYSTEMOWNER.EMAIL}} |

## Authorizing Official

**Senior management official designated as the authorizing official:**

|  |  |
| --- | --- |
| Name: | {{SSP|SECURITYPLAN.PLANAUTHORIZINGOFFICIAL.FULLNAME}} |
| Title: | {{SSP|SECURITYPLAN.PLANAUTHORIZINGOFFICIAL.JOBTITLE}} |
| Office Address: | {{SSP|SECURITYPLAN.PLANAUTHORIZINGOFFICIAL.COMPANY}}  {{SSP|SECURITYPLAN.PLANAUTHORIZINGOFFICIAL.ADDRESS}} |
| Work Phone: | {{SSP|SECURITYPLAN.PLANAUTHORIZINGOFFICIAL.WORKPHONE}} |
| e-Mail Address: | {{SSP|SECURITYPLAN.PLANAUTHORIZINGOFFICIAL.EMAIL}} |

## Information System Security Officer

**Assignment of security responsibility:**

|  |  |
| --- | --- |
| Name: | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.FULLNAME}} |
| Title: | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.JOBTITLE}} |
| Office Address: | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.COMPANY}}  {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.ADDRESS}} |
| Work Phone: | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.WORKPHONE}} |
| e-Mail Address: | {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.EMAIL}} |

## Information System Operational Status

{{SSP|SECURITYPLAN.STATUS}}

## Information System Type

{{SSP|SECURITYPLAN.SYSTEMTYPE}}

## General Description and Purpose

**Description:**

{{SSP|SECURITYPLAN.DESCRIPTION}}

**Purpose:**

{{SSP|SECURITYPLAN.PURPOSE}}

**Environment:**

{{SSP|SECURITYPLAN.ENVIRONMENT}}

**Laws and Regulations:**

{{SSP|SECURITYPLAN.LAWSANDREGULATIONS}}

## Authorization Boundary

A detailed and explicit definition of the system authorization boundary diagram is represented in the Authorization Boundary Diagram below.

{{TEXTBOX|SECURITYPLAN.AUTHORIZATIONBOUNDARY}}

## User Roles

{{TABLE|USERS}}

**Roles of Users and Number of Each Type:**

|  |  |
| --- | --- |
| **Number of Users** | **Number of Administrators/**  **Privileged Users** |
| {{SSP|SECURITYPLAN.USERS}} | {{SSP|SECURITYPLAN.PRIVILEGEDUSERS}} |

## Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity, and availability sensitivity levels.

The following tables identify the information types that are transmitted, stored, and/or processed by the {{SSP|SECURITYPLAN.OTHERIDENTIFIER}}. The selection of the information types is based on guidance provided by Federal Information Processing Standard (FIPS) Pub 199, Standards for Security Categorization of Federal Information and Information Systems and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

{{TABLE|2-2}}

# SYSTEM ENVIRONMENT

The logical network topology is shown in the figure below. The diagram provides a visual depiction of the system network components that constitute {{SSP|SECURITYPLAN.OTHERIDENTIFIER}}.

{{TEXTBOX|SECURITYPLAN.NETWORKARCHITECTURE}}

## Hardware Inventory

The figures below provide a listing of all hardware components associated with the system.

{{TABLE|HARDWARE}}

## Software Inventory

The figure below provides a listing of all software components associated with the system.

{{TABLE|SOFTWARE}}

## System Interconnections/Information Sharing

The table below list the systems that are interconnected with the {{SSP|SECURITYPLAN.OTHERIDENTIFIER}}.

{{TABLE|11-1}}

## Data Flow

The data flow in and out of the system boundary is depicted in the diagram below.

{{TEXTBOX|SECURITYPLAN.DATAFLOW}}

## Ports, Protocols and Services

The table below lists the ports, protocols, and services enabled within the information system.

{{TABLE|10-1}}

# MINIMUM SECURITY CONTROLS

Security controls must meet minimum security control baseline requirements. Upon categorizing a system as Low, Moderate, or High sensitivity in accordance with FIPS 199, the corresponding security control baseline standards apply. Security controls that are representative of the sensitivity of the {{SSP|SECURITYPLAN.OTHERIDENTIFIER}} are described in the sections that follow.

{{CONTROLS}}

# SYSTEM SECURITY PLAN APPROVAL

## System Security Plan Completion Date

{{SSP|SECURITYPLAN.FEDRAMPDATESUBMITTED}}

## System Security Plan Approval Date

{{SSP|SECURITYPLAN.PLANAUTHORIZINGOFFICIAL.FULLNAME}}

{{SSP|SECURITYPLAN.PLANAUTHORIZINGOFFICIAL.JOBTITLE}}

{{SSP|SECURITYPLAN.FEDRAMPDATEAUTHORIZED}}

# RECORD OF CHANGES

|  |  |  |
| --- | --- | --- |
| Date | Description | Made By: |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |