**System Security Plan**

For the {{SSP|SECURITYPLAN.SYSTEMNAME}} System

Approved by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

{{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.FIRSTNAME}} {{SSP|SECURITYPLAN.PLANINFORMATIONSYSTEMSECURITYOFFICER.LASTNAME}}

Information System Security Officer

Approved by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

{{SSP|SECURITYPLAN.SYSTEMSECURITYMANAGER.FIRSTNAME}} {{SSP|SECURITYPLAN.SYSTEMSECURITYMANAGER.LASTNAME}}

Information System Security Manager

Approved by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

{{SSP|SECURITYPLAN.SYSTEMOWNER.FIRSTNAME}} {{SSP|SECURITYPLAN.SYSTEMOWNER.LASTNAME}}

System Owner

Approved by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

{{SSP|SECURITYPLAN.PLANAUTHORIZINGOFFICIAL.FIRSTNAME}} {{SSP|SECURITYPLAN.PLANAUTHORIZINGOFFICIAL.LASTNAME}}

Authorizing Official Designated Representative

Effective Date: {{SSP|SECURITYPLAN.DATECREATED}}

Table of Contents

[List of Figures 3](#_Toc111450453)

[List of Tables 3](#_Toc111450454)

[Revision Summary 4](#_Toc111450455)

[Executive Summary 5](#_Toc111450456)

[Acronym List 6](#_Toc111450457)

[1.0 SYSTEM IDENTIFICATION 7](#_Toc111450458)

[2.0 organizational role assignment 7](#_Toc111450459)

[3.0 OPERATIONAL STATUS 7](#_Toc111450460)

[4.0 GENERAL DESCRIPTION/PURPOSE 7](#_Toc111450461)

[5.0 MISSION CRITICALITY 8](#_Toc111450462)

[6.0 SYSTEMS DESCRIPTION AND BOUNDARY IDENTIFICATION 8](#_Toc111450463)

[7.0 SYSTEM INTERCONNECTIONS 9](#_Toc111450464)

[8.0 SYSTEM CATEGORIZATION 9](#_Toc111450465)

[9.0 REFERENCES 11](#_Toc111450466)

[10.0 ATTACHMENTS 11](#_Toc111450467)

List of Figures

Figure 1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Authorization Boundary Diagram 8

Figure 2. {{SSP|SECURITYPLAN.SYSTEMNAME}} Network Architecture Diagram 8

Figure 3. {{SSP|SECURITYPLAN.SYSTEMNAME}} Data Flow Diagram 8

List of Tables

Table 1. {{SSP|SECURITYPLAN.SYSTEMNAME}} System Identification 7

Table 2. Organizational Role Assignment 7

Table 3. Security Categorization of Management and Support Information Table for the {{SSP|SECURITYPLAN.SYSTEMNAME}} 10

Revision Summary

|  |  |  |  |
| --- | --- | --- | --- |
| Rev. No. | Description of Change | Pages | Date |
| 0 |  | All |  |

Executive Summary

{{TEXTBOX|SECURITYPLAN.EXECUTIVESUMMARY}}

Acronym List

|  |  |
| --- | --- |
| CIA | Confidentiality, Integrity, and Availability |
| CoL | Consequence of Loss |
| CSOS | Cyber Security Oversight System |
| CSPP | Cyber Security Program Plan |
| DMZ | Demilitarized Zone |
| DOE | U.S. Department of Energy |
| FIPS | Federal Information Processing Standard |
| GSS | General Support System |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| O | Order |
| PPPO | Portsmouth/Paducah Project Office |
| SIEM | Security Information and Event Management |
| SP | Special Publication |
| SSP | System Security Plan |
| UCI | Unclassified Controlled Information |
| VPN | Virtual Private Network |

# SYSTEM IDENTIFICATION

Table 1. {{SSP|SECURITYPLAN.SYSTEMNAME}} System Identification

|  |  |
| --- | --- |
| System Name: | {{SSP|SECURITYPLAN.SYSTEMNAME}} |
| System Type: | {{SSP|SECURITYPLAN.SYSTEMTYPE}} |
| System Status: | {{SSP|SECURITYPLAN.STATUS}} |
| Authority to Operate Status: | {{SSP|SECURITYPLAN.FEDRAMPAUTHORIZATIONSTATUS}} |
| Responsible Organization: | {{SSP|SECURITYPLAN.PREPORGNAME}} |
| System Location(s): | {{SSP|SECURITYPLAN.PREPADDRESS}} {{SSP|SECURITYPLAN.PREPCITYSTATE}} |

# organizational role assignment

Table 2. Organizational Role Assignment

{{DOETABLE|DOEUSERS}}

For specific information related to all of the roles and responsibilities for the {{SSP|SECURITYPLAN.SYSTEMNAME}} System, refer to the {{SSP|SECURITYPLAN.SYSTEMNAME}} Systems Cyber Security Policy, the {{SSP|SECURITYPLAN.SYSTEMNAME}} System Roles and Responsibilities Matrix, the {{SSP|SECURITYPLAN.SYSTEMNAME}} System Cyber Security Procedure, and the {{SSP|SECURITYPLAN.SYSTEMNAME}} System Development Life-Cycle Plan.

# OPERATIONAL STATUS

The {{SSP|SECURITYPLAN.SYSTEMNAME}} System is currently in the **{{SSP|SECURITYPLAN.STATUS}}** Phase.

# GENERAL DESCRIPTION/PURPOSE

{{TEXTBOX|SECURITYPLAN.DESCRIPTION}}

{{TEXTBOX|SECURITYPLAN.PURPOSE}}

# MISSION CRITICALITY

The CSOS **is not** categorized as a DOE mission-critical system.

# SYSTEMS DESCRIPTION AND BOUNDARY IDENTIFICATION

{{SSP|SECURITYPLAN.AUTHORIZATIONBOUNDARY}}

Figure 1. {{SSP|SECURITYPLAN.SYSTEMNAME}} Authorization Boundary Diagram

{{SSP|SECURITYPLAN.NETWORKARCHITECTURE}}

Figure 2. {{SSP|SECURITYPLAN.SYSTEMNAME}} Network Architecture Diagram

{{SSP|SECURITYPLAN.DATAFLOW}}

Figure 3. {{SSP|SECURITYPLAN.SYSTEMNAME}} Data Flow Diagram

# SYSTEM INTERCONNECTIONS

{{DOETABLE|DOEINTERCONNECTS}}

# SYSTEM CATEGORIZATION

{{SSP|SECURITYPLAN.CATEGORIZATIONJUSTIFICATION}}

.

All systems within the {{SSP|SECURITYPLAN.SYSTEMNAME}} boundary conform to the management and operational controls specified in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, for the appropriate level of CIA-related risk required to protect the information and information system.

Table 3 describes the information system categorization. For an information system, the potential impact values assigned to the respective security objectives C, I, and A shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information that resides on the information system.

Table 3. Security Categorization of Management and Support Information

Table for the {{SSP|SECURITYPLAN.SYSTEMNAME}}

{{DOEMIXTABLE|DOECLASSIFICATIONTABLE}}

The overall Categorization level for this boundary is {{SSP|SECURITYPLAN.OVERALLCATEGORIZATION}}.

# REFERENCES

Standards and Guidance

{{DOETABLE|DOESTANDARDSGUIDANCE}}

Laws and Regulations

{{DOETABLE|DOELAWSREGULATIONS}}

# ATTACHMENTS

Attachment 1, Security Control Catalog

Attachment 1

Security control catalog

This section contains the security control catalog identifying security controls selected for implementation from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. The following table contains descriptions of fields in the control catalog and the associated values.

| **Security Control Field Description** | |
| --- | --- |
| **Field** | **Description** |
| Control ID | The primary control identifier |
| Name | The full name of the control |
| Requirement | The identified requirement |
| Source | The following are definitions of values in this column:  B – The control is identified in the baseline selected from NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations determined by the categorization (e.g., low, moderate, high) of the information system.  I – The control has been inherited from an information system providing the security functionality as a common control. The information system the control is inherited from is identified in the implementation field.  O – The control is implemented as part of an overlay developed by the site, Headquarters, a government-wide organization, or a vendor. Controls from overlays will be fully documented within the System Security Plan (SSP) itself and not simply reference the source overlay.  T – The control has been tailored in or out of the controls selected for the information system based on an assessment of risk, operational requirements, and/or a cost/benefit analysis. Additional information regarding the control tailoring decision is found in the notes field. |
| Type | C – The control is provided as a common control and inheritable by other information systems.  S – The control is system-specific and the responsibility for its management and operations are that of the organization that implemented it.  H – A hybrid control is partially inherited from another information system providing it as a common control and partially system-specific and implemented by the organization. |
| Status | The following are definitions of values in this column:  I – The security control is implemented per the specification.  N – The security control is not implemented per the specification.  R – Risk Accepted |
| Implementation | This field contains the organization-specific implementation of the security control. |
| Note | Notes about the implementation, non-implementation, or references. |

{{DOECONTROLS}}