[Insert System Name Here]

System Security Plan

Security Categorization: [Level Here]

{DATE}

Version {x.x}

Prepared by:

Table of Contents

Executive Summary

State of Ohio agencies are required to identify each information system that contains, processes, and transmits state data and information and to prepare and implement a plan for the security and privacy of these systems. The objective of system security planning is to improve protection of information technology (IT) resources. All State of Ohio systems have some level of sensitivity, and require protection as part of best management practices. The protection of a system must be documented in a system security plan. The security plan is viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It reflects input from management responsible for the system, including information owners, the system operator, the system security manager, and system administrators.

This System Security Plan (SSP) provides an overview of the security requirements for **<System Name>** and the associated controls document describes the controls in place or planned for implementation to provide a level of security appropriate for the information processed as of the date indicated.

Note: The SSP is a living document that will be updated periodically to incorporate new and/or modified security. The plan will be revised as the changes occur to the system, the data or the technical environment in which the system operates.

Change/Review Record

This **[Insert System Name Here]** System Security Plan (SSP) is a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to this document are recorded in the Change/Review Record below. Reviews made as part of the assessment process should also be recorded below. This history shall be maintained throughout the life of the document.

Version Number	Date	Description of Change/Revision	Section/Pages Affected	Changes Made by Name/Title/ Organization
1.0	**[Insert Update Date Here]**	Template Created	All	**[Insert Name/Title/Team]**

System Security Plan Approval Signatures

I have reviewed the **[Insert System Name Here]** System Security Plan and accept the analysis and findings within.

_____ _____

[Insert Name Here] Date

System Owner

1. Information System Name/Title:

- Unique identifier and name given to the system.

2. Information System Categorization/Security Risks and Concerns:

- To identify the information system categorization in reference with FIPS-199. The information gathered from the data classification and risk assessment will provide the details necessary to select the appropriate level.

	LOW		**MODERATE**		**HIGH**

- Please provide describe the security risks and concerns within this section.

3. Information System Owner:

- Name, title, agency, address, email address, and phone number of person who owns the system.

4. Authorizing Official:

- Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.

5. Other Designated Contacts:

- List other key personnel, if applicable; include their title, address, email address, and phone number.

6. Assignment of Security Responsibility:

- Name, title, address, email address, and phone number of person who is responsible for the security of the system.

7. Information System Operational Status:

- Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

	Operational		**Under Development**		**Major Modification**

8. General System Description/Purpose

- Describe the function or purpose of the system and the information processes.

9. System Environment

- Provide a general description of the technical system. Include the primary hardware, software, communications equipment, infrastructure architecture, security processes.

- Detail the technical specifics to satisfy the following Network segmentation, Perimeter security, Application security and data sensitivity classification, PHI and PII data elements, Intrusion management, Monitoring and reporting, Host hardening, Remote access, Encryption, State-wide active directory services for authentication, Interface security, Security test procedures, Managing network security devices, Security patch management, Detailed diagrams depicting all security-related devices and subsystems and their relationships with other systems for which they provide controls and Secure communications over the Internet.

10. System Interconnections/Information Sharing

- List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.

System Name	Organization	Type	Agreement (ISA/MOU/MOA)	Date of Agreement	Categorization Level

11. Related Laws/Regulations/Policies/Guidelines

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

12. Security Controls Document – <u>Attachment A of System Security Plan</u>

Please provide a controls document with the appropriate selection of a minimum or in place security control baseline based on the system categorization (low, moderate, and high-impact) or tailored controls in the organizations framework format (NIST SP 800-53, ISO27001, COBIT, etc.).

The document must contain a thorough description of how all the minimum or in place security controls within the applicable baseline or control tailoring are being implemented or planned to be implemented.

The description should contain:

- Security control title
- How the security control is being implemented or planned to be implemented.
- Any scoping guidance that has been applied and what type of consideration.
- Indicate if the security control is a common control and who is responsible for its implementation.
- Logical security controls (privacy, user access and authentication, user permissions, etc.)
- Technical security controls and security architecture (communications, hardware, data, physical access, software, operating system, encryption, etc.)

13. Information System Security Plan Completion Date: _____

- Enter the completion date of the plan.

14. Information System Security Plan Approval Date: _____

- Enter the date the system security plan was approved by the system owner and indicate if the approval documentation is attached or on file.

15. Security System/Project Deliverables

- Enter Please list the security specific project deliverables within this section.

16. Attachment (A) – Security Controls Document