

<Project Name>

System Security Plan

**Version: <Type Version #>**

**Date:**

**My signature indicates approval of this System Security Plan.**

**Prepared by:**

Project Manager

**Approved by:**

Project Sponsor

**Approved by:**

Agency CIO

**Approved by:**

Executive Sponsor

**Table of Contents**

[1 PURPOSE 3](#_Toc106979598)

[2 APPLICABILITY AND RENEWAL 3](#_Toc106979599)

[3 EXEMPTIONS 3](#_Toc106979600)

[4 MANDATE AND REFERENCES 3](#_Toc106979601)

[5 DEFINITIONS 3](#_Toc106979602)

[6 AUTHORIZATION PROCESS 4](#_Toc106979603)

[7 APPENDIX A: INSTRUCTIONS 4](#_Toc106979604)

[8 APPENDIX B: SYSTEM SECURITY PLAN TEMPLATE 7](#_Toc106979605)

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| <MM/DD/YYYY> | <0.00> | <Type brief description here> | <First Initial & Last Name> |
|  |  |  |  |

**Template Overview and Instructions:**

Please read the entire document and fill out as directed for a full understanding of the security requirements by DoIT to ensure confidentiality, integrity, and availability of State Information Technology (IT) networks, systems, and applications.

# PURPOSE

The State of Maryland Department of Information Technology (DoIT) Cybersecurity Authority to Operate Policy requires agencies to undergo a standardized process for approval for new devices, networks, or applications. To maintain a strong security posture and assure the confidentiality, integrity, and availability of State Information Technology (IT) networks, systems, and applications, all devices and networks must comply with security policies and configuration standards before they are approved to operate in State IT environments.

Personnel seeking to implement a new device, network, or application (collectively referred to as “information systems and connections”) must fill out a **System Security Plan (SSP)** as provided in Appendix B and provide that to the proper **Designated Approval Authority (DAA)**. Instructions on how to fill out the SSP document are provided in Appendix A. Dependent upon the information provided in the SSP and verified through a Risk Management Process – more information may be requested; more security controls may be required, or an information system may be granted an **Authority to Operate (ATO)** or **Interim Authority to Operate (IATO)** accreditation.

# APPLICABILITY AND RENEWAL

This policy is applicable to all IT environments and assets utilized by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology. DoIT will be responsible for determining whether devices are authorized to operate and for ensuring the authorization state of all such devices and networks for onboarded Agencies is being tracked. Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy.

No new device, network, or application (collectively referred to as “information systems and connections”) shall be permitted to operate without a risk assessment and a signed ATO or IATO form. ATO’s are granted for a default time of three (3) years, after which a new **System Security Plan (SSP)** must be completed for the authorized entity, system, or connection. IATO’s may be granted for a maximum time of six (6) months.

# EXEMPTIONS

A System Security Plan is required for all information systems and connections, unless an ATO or IATO has been granted for an information system configuration standard that has been evaluated in a prior SSP. If an agency wishes to receive an exemption from the SSP requirement, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks. If the agency can accept the risk, an exemption to this requirement may be granted.

# MANDATE AND REFERENCES

*The DoIT Cybersecurity Authority to Operate Policy mandates this document.*

# DEFINITIONS

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Authority to Operate (ATO) | Authority granted to an information system, by a Designated Approving Authority (DAA), to be used in accordance with its intended purpose within agency IT environments. An ATO authorizes operation of a Business Product and explicitly accepts the risk to agency operations. |
| Designated Approval Authority (DAA) | Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Responsible for signing Authority to Operate (ATO), Interim Authority to Operate (IATO), and associated Third-Party Interconnection Agreements. |
| FIPS 199 | Guidance which helps classify assets based on the intensity of a potential impact that may occur if the information system is jeopardized. |
| Interim Authority to Operate (IATO) | Temporary authority granted to an information system to be used in accordance with its intended purpose within agency IT environments. IATOs are used to permit information systems to operate although non-compliant with some agency security policies or requirements, so long as the information system is brought into compliance within a designated time. |
| System Development Life Cycle (SDLC) | The scope of activities associated with a system, encompassing the system’s initiation, development and acquisition, implementation, operation, and maintenance, and ultimately its disposal that instigates another system initiation. |
| System Security Plan (SSP) | Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. |

# AUTHORIZATION PROCESS

Any employee found to have violated this requirement may be subject to disciplinary action, up to and including termination of employment. Devices or networks found to be in operation without an ATO or IATO or found to be in violation of the terms under which the ATO or IATO were granted, may be subject to immediate deactivation or disconnection from other agency environments and third parties.

# APPENDIX A: INSTRUCTIONS

Agencies or personnel wishing to implement new information systems and connections must complete the System Security Plan template (Appendix B) for each asset or standardized configuration. For reference, a standardized configuration may be applied to a class of assets that will be configured by the same build (e.g., user desktop environment may be installed with a standardized Windows 7 operating system image that has no specialized purpose, while Windows servers may be thought of as standardized if each server will be configured with a specialized purpose (such as a Domain Controller, Backup server, DNS server, etc.) and must be individually identified).

Instructions related to each question on the form are described below. Please contact DoIT Security Services with any questions or concerns. # Information Instruction.

|  |  |  |
| --- | --- | --- |
| **#** | **Information** | **Instruction** |
| 1 | System Name | Each system should be assigned a name and unique identifier by the Agency. This unique name and identifier supports the traceability of the system and correlates to audit logs related to system use. |
| 2 | Categorization | Each system must be categorized using **FIPS 199**. NIST SP 800-60*, Guide for Mapping Types of Information and Information Systems to Security Categories*, provides implementation guidance in completing this activity. |
| 3 | Information System Owner | Each system must have a designated system owner that serves as the key point of contact (POC) for the system and is responsible for following a **system development life cycle (SDLC)**.   Please fill out all the contact information identified in the form. |
| 4 | Authorizing Official | Contact information for authorizing official must be identified in the system security plan for each system. This person serves as a senior management official who has the authority to authorize and accept the residual risk associated with the system. This person may be the:   Agency’s Deputy CIO; or   Director of Cybersecurity/State CISO or designated official (if agency IT or security decisions are handled by DoIT) |
| 5 | Other Designated Contact | Contact information for other key contact personnel who can address inquiries regarding the system and operation. |
| 6 | Assignment of Security | Responsibility Contact information for an individual assigned responsibility for each system. |
| 7 | System Operational Status | Indicate the system’s operational status:   *Operational* – the system is in production.   *Under Development* – the system is being designed, developed, or implemented; or   *Undergoing a Major Modification* – the system is undergoing a major conversion or transition. |
| 8 | Information System Type | Indicate whether the system is either a:   *Major Application* – defined as an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.   *General Support System* – defined as an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. |
| 9 | General System Description/Purpose | Provide a brief description of the function and purpose of the system (e.g., network support, data analysis, web development.)   NOTE: If the system is a general support system, list all applications supported by the general support system. |
| 10 | System Environment | Provide a brief general description of the technical system. Include the primary hardware, software, and communications equipment. |
| 11 | System Interconnections | Identify all system interconnections, defined as a direct connection of two or more IT systems for the purposes of sharing information.   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 name of authorizing official. |
| 12 | Related Law, Regulations, Policies | List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, and availability of the system and information retained by, transmitted by, or processed by the system (e.g., HIPAA, IRS 1075, PCI DSS). |

# APPENDIX B: SYSTEM SECURITY PLAN TEMPLATE

**1.** **Information System Name/Title:**

**2. Information System Categorization:**

*Please toggle relevant category.*

|  |  |
| --- | --- |
| Low |  |
| Moderate |  |
| High |  |

**3. Information System Owner:**

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Agency |  |
| Address |  |
| Email Address |  |
| Phone Number |  |

**4. Authorizing Official:**

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Agency |  |
| Address |  |
| Email Address |  |
| Phone Number |  |

**5. Other Designated Contacts:**

|  |  |
| --- | --- |
| Alternate Contact #1: |  |
| Alternate Contact #2: |  |

**6. Assignment of Security Responsibility:**

|  |  |
| --- | --- |
| Name |  |
| Title |  |
| Agency |  |
| Address |  |
| Email Address |  |
| Phone Number |  |

**7. Information System Operational Status:**

*Please toggle relevant category.*

|  |  |
| --- | --- |
| Operational |  |
| Under Development |  |
| Major Modification |  |

**8. Information System Type:**

*Please toggle relevant category.*

|  |  |
| --- | --- |
| Major Application |  |
| General Support System |  |

**9. General System Description/Purpose:**

Type here

**10. System Environment:**

Type Here

**11. System Interconnections/Information Sharing:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **System Name** | **Organization** | **System Type** | **Agreement** | **Date** | **FIPS 199 Category** | **C&A Status** | **Authorizing Official** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**12. Related Laws, Regulations, or Policies:**

**NEXT STEPS:**

Please provide electronic copies of completed SSP documents to the DoIT Security Team. The DoIT Security Team will analyze the proposed system for relevant STIGS and security measures. Upon completion of the initial analysis of the SSP, the DoIT Security Team may call a meeting with the relevant system owners/stakeholders to discuss detailed security controls and configurations that will be required of the proposed system. System owners will then be required to provide **security control documentation** that asserts: (1) an assurance that the system will meet security requirements or (2) a justification and mitigation for security requirements that cannot be currently met. An examination of the SSP document and the security control documentation, by the DoIT Security Team, will determine whether a system is granted the following:

* Authority to Operate (ATO)
* Interim Authority to Operate (IATO)
* Denied