# Information System Security Plan Template

Every agency information system must have a unique name and identifier. Assignment of a unique ID supports the agency's ability to collect asset information and security metrics.

**Information System Name:**

**Information System ID:**

Every agency information system must be categorized using FIPS 199
http://doit.maryland.gov/support/Documents/security_guidelines/Security_Categorization.pdf
If the system processes or stores confidential information, it shall be categorized 'Moderate' at minimum.

**System Categorization:** LOW MODERATE HIGH

**Information System Owner:** This person is the key point of contact for the system and is responsible for coordinating system development life cycle (SDLC) activities specific to the system.

Name
Title
Agency
Address
e-mail
Phone

**Authorizing Official:** This person is the senior management official who has the authority to authorize operation (accredit) of this system and accept the residual risk associated with it.

Name
Title
Agency
Address
e-mail
Phone

**System Security Control Monitor:** This person is responsible for monitoring and maintaining the security controls described in this plan.

Name
Title
Agency
Address
e-mail
Phone

**Information System Operational Status:**
Operational Under Development Major Modification

**Information System Type:** Major Application General Support

**General System Description/Purpose:** Describe the function or purpose of the system.

**System Environment:** Provide a general description of the technical system. Include the primary hardware, operating system, applications and data flow.

**System Interconnections/Information Sharing:** List interconnected systems and identifiers.

| System Name | Agency | System Categorization |
|---|---|---|

**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.

**Minimum Security Controls:**
Select the appropriate minimum security control baseline (Low-, Moderate-, High-impact) from NIST SP 800-53 http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf then provide a thorough description of how all the minimum security controls in the applicable baseline are being implemented or plan to be implemented. *Managerial and Operational security controls may be inherited (and documented) at the agency level.*

**Moderate-Level System Technical Security Controls;**

| **Security Control** | **Y/N** | **Explanation of how control is implemented including who is responsible for it** |
|---|---|---|
| Are user account access privileges managed? | | |
| Can the system enforce assigned authorizations that control system access and the flow of information within the system and between interconnected systems? | | |
| Are procedures in place to ensure that only authorized individuals can access confidential information residing within the system? | | |
| Have specific user actions that can be performed on the system without identification or authentication been identified? | | |
| Can the system enforce separation of duties through assigned access authorizations? | | |
| Can the system enforce the most restrictive access capabilities required for specified tasks? | | |
| Has an account lock-out policy been implemented within the system? | | |
| Has a warning banner been applied for all modules of the system that receive, store, process and transmit confidential information? | | |
| Has an account time-out policy been implemented within the system? | | |
| Have all remote access capabilities to the system been authorized and documented? | | |

|  |  |  |
|---|---|---|
| Have formal procedures been developed that define how authorized individuals may access the system from external systems? |  |  |
| Have wireless access procedures (to the system) been developed? |  |  |
| Are restrictions in place to prevent unauthorized devices from accessing the system? |  |  |
| Has the system been configured to generate audit records for all security-relevant events, including all security and system administrator accesses? |  |  |
| Has system auditing been enabled to capture access, modification, deletion and movement of confidential information by each unique user? |  |  |
| Has the system been configured to alert appropriate agency officials in the event of an audit processing failure and/or take additional actions? |  |  |
| Has the system been configured to allocate sufficient audit record storage capacity to record all necessary auditable items? |  |  |
| Has the system been configured to produce audit records that contain sufficient information to, at a minimum establish; (i) what type of event occurred, (ii) when (date and time) the event occurred, (iii) where the event occurred, (iv) the source of the event, (v) the outcome (success or failure) of the event, (vi) the identity of any user/subject associated with the event? |  |  |
| Have procedures been developed to routinely review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to appropriate officials? |  |  |

| | | |
|---|---|---|
| Has the system been configured to automatically process audit records for events of interest based on selectable event criteria and also provide report generation capabilities? | | |
| Has an audit record retention policy been implemented within the system? | | |
| Has the system been configured to protect audit information and audit tools from unauthorized access, modification, and deletion? | | |
| Has the system been configured to uniquely identify users, devices, and processes via the assignment of unique user accounts and validate users (or processes acting on behalf of users) using standard authentication methods such as passwords, tokens, smart cards, or biometrics? | | |
| Have system user account management procedures been developed to include (i) obtaining authorization from appropriate officials to issue user accounts to intended individuals; (ii) disabling user accounts in a timely manner; (iii) archiving inactive or terminated user accounts; and (iv) developing and implementing standard operating procedures for validating system users who request reinstatement of user account privileges suspended or revoked by information systems? | | |
| Has the system been configured to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals? | | |

| | | |
|---|---|---|
| Have approved cryptographic modules been implemented to protect confidential information? | | |
| Has the system been configured to prevent residual data from being shared with, recovered, or accessed by unauthorized users (or processes acting on behalf of users) once such data is removed from the information system and the memory once occupied by such data is reallocated to the information system for reuse, as applicable? | | |
| Have front end system interfaces been separated from back end processing and data storage? | | |
| Has the system been configured to prevent unauthorized and unintended information transfer via shared system resources? | | |
| Has the system been configured to monitor and control communications at all external boundaries of the system and at key internal boundaries within the system? | | |
| Have procedures been implemented to protect the confidentiality of confidential information during electronic transmission? | | |
| Have cryptographic key management procedures been implemented? | | |
| Has an external network connection time-out policy been implemented within the system? | | |

**Completion Date:**

**Approval Date:**