|  |  |  |
| --- | --- | --- |
|   | Information System Security Plan  |   |

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

Unique identifier and name given to the system.

**2. Security Categorization (SC) Applied to Information TYPES:**

Identify the appropriate [FIPS 199](http://csrc.nist.gov/publications/PubsFIPS.html) categorization.

**SC information type** = {(confidentiality, *impact*),(integrity, *impact*),(availability, *impact*)}

Acceptable values for potential impact are LOW, MODERATE, HIGH, or N/A (confidentiality only)

Refer to Table 1 for the Potential Impact Matrix.

**3. Security Categorization (SC) Applied to Information SYSTEMS:**

Identify the appropriate [FIPS 199](http://csrc.nist.gov/publications/PubsFIPS.html) categorization.

**SC information system** = {(confidentiality,impact),(integrity,impact),(availability,impact)}

Acceptable values for potential impact are LOW, MODERATE or HIGH. N/A is not an option!

Refer to Table 1 for the Potential Impact Matrix.

**4. Information System Owner:**

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

**5. Authorizing Official:**

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

**6. Other Designated Contacts:**

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

**7. Assignment of Security Responsibility:**

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

**8. 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

**9. Information System Type:**

Indicate if the system is a:

* Major application
* General support system

If the system contains minor applications, list them in Section 10 - General System Description/Purpose.

**10. General System Description/Purpose**

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

**11. System Environment**

Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.

**12. System Interconnections/Information Sharing**

List interconnected systems and system identifiers (if appropriate):

1. System name
2. Organization
3. System type (major application or general support system)
4. Indicate if there is an SLA/MOU or other agreement on file
5. Date of agreement to interconnect
6. FIPS 199 category
7. The name of the authorizing official

**13. 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.

**14. Minimum Security Controls**

Select the appropriate minimum security control baseline (low-, moderate-, high-impact) from [NIST SP 800-53](http://csrc.nist.gov/publications/PubsSPs.html), then provide a thorough description of how all the minimum security controls in the applicable baseline are being implemented or planned to be implemented. The description should contain:

1. The security control title
2. How the security control is being implemented or planned to be implemented
3. Any scoping guidance that has been applied and what type of consideration
4. Indicate if the security control is a common control and who is responsible for its implementation

**15. Information System Security Plan Completion Date**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Enter the completion date of the plan.

**16. Information System Security Plan Approval Date**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

|  |
| --- |
| POTENTIAL IMPACT |
| Security Objective | LOW | MODERATE | HIGH |
| Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]  | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.  | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.  | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.  |
| Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]  | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.  | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.  | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.  |
| Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]  | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.  | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.  | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.  |

Table 1: Potential Impact Definitions for Security Objectives