

SECTION J

ATTACHMENT J-3: INFORMATION SYSTEM SECURITY PLAN TEMPLATE

Insert Company Name

Information System Security Plan

This document is a template and should be completed per guidance provided by the requirements listed in Section 2 below. Areas in italics or highlighted must be completed.

Review and Approvals

REVIEWED BY:

Information System Owner
Typed First/Last Name

Date

EMCBC Information System Security Manager (ISSM)
John Muskoff

Date

WVDP Federal Project Manager
Typed First/Last Name

Date

APPROVED BY:

EMCBC Authorizing Official Designated
Representative (AODR)
Ward E. Best, EMCBC ADIRM

Date

Completion Date: _____

Effective Date: _____

DRAFT

System Security Plan

1. Purpose:

The purpose of the System Security Plan (SSP) is to define system components, operational boundaries, and roles and responsibilities for managing the system.

2. Requirements and Guidance:

- Federal Information Security Management Act (FISMA) 2002
- OMB Circular 130-A, Management of Federal Information Resources
- NIST Special Publication 800-53, Rev 4 – Security and Privacy Controls for Federal Information Systems and Organizations
- DOE Cyber Security Program, DOE O 205.1B
- NIST Special Publication 800-61, Rev 2 – Computer Security Incident Handling Guide
- NIST Special Publication 800-128 – Guide for Security-Focused Configuration Management of Information Systems
- NIST Special Publication 800-18, Rev 1 - Guide for Developing Security Plans for Federal Information Systems
- NIST Special Publication 800-30, Rev 1 - Guide for Conducting Risk Assessments
- NIST Special Publication 800-37 – Guide for Applying Risk Management Framework to Federal Information Systems
- NIST Special Publication 800-100 – Information Security Handbook: A Guide for Managers
- NIST FIPS-199 Standards for Security Categorization of Federal Information and Information Systems

3. Information System Name/Title:

- **ABC Company, Inc.** General Support System (GSS)

4. Information System Type:

- Indicate if the system is a major application or a General Support System. If the system contains minor applications, list them in Section 9. General System Description/Purpose. *(This should be a General Support System comprised of several individual stand-alone systems).*

<input type="checkbox"/>	Major Application	<input type="checkbox"/>	General Support System
--------------------------	--------------------------	--------------------------	-------------------------------

5. Information System Categorization:

- Identify the appropriate system categorization using FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. *(Categorizations below are examples and should be changed as necessary.)*

System Name	Confidentiality	Integrity	Availability	Interconnection
ABC Inc. GSS	Low	Low	Low	None

6. Information System Owner:

- Position with responsibility for the information system. (**Note:** This document should only reflect roles by position, not individual names. Assignment of roles by name is done through an Appointments Memorandum, which can be changed without a formal review process, unlike the SSP.)

7. Authorizing Official:

EMCBC Authorizing Official Designated Representative (AODR):
 Ward E. Best, EMCBC Assistant Director, Information Resource Management (ADIRM)

8. Assignment of Roles and Responsibilities:

- List roles and associated responsibilities (*Contracting Officer's Representative (COR), Authorizing Official (AO), Information System Security Officer (ISSO), Information System Security Manager (ISSM), Information System Owner (ISO), and other roles as applicable per NIST SP 800-18 Rev 1. This table is only a reference and can be removed or modified as necessary.*)

Title	Assigned To	Responsibilities
Contracting Officer's Representative (COR)	COR	<ul style="list-style-type: none"> Agency Project Manager providing direction and guidance to Contractor Assists COR with regard to contractual matters
DOE Authorizing Official (AO)	AO	<ul style="list-style-type: none"> DOE official approving system security plans, Authorizes operation of an information system, Issues an interim authorization to operate the information system under specific terms and conditions, or Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.
Information Owner	CIO	<ul style="list-style-type: none"> Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior),⁷ Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides, Decides who has access to the information system and with what types of privileges or access rights, and

		<ul style="list-style-type: none"> Assists in the identification and assessment of the common security controls where the information resides.
Information System Security Manager (ISSM)	CIO	<ul style="list-style-type: none"> Carries out DOE responsibilities for system security planning, Coordinates the development, review, and acceptance of system security plans with information system owners, information system security officers, and the authorizing official, Coordinates the identification, implementation, and assessment of the common security controls, and Possesses professional qualifications, including training and experience, required to develop and review system security plans.
Information System Security Officer (ISSO)	System Administrator	<ul style="list-style-type: none"> Assists the senior agency information security officer in the identification, implementation, and assessment of the common security controls, and Plays an active role in developing and updating the system security plan as well as coordinating with the information system owner any changes to the system and assessing the security impact of those changes.
Contractor Information System Owner (ISO)	CIO	<ul style="list-style-type: none"> Develops the system security plan in coordination with information owners, the system administrator, the information system security officer, the senior agency information security officer, and functional "end users," Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements, Ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior), Updates the system security plan whenever a significant change occurs, and Assists in the identification, implementation, and assessment of the common security controls.

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

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

10. System Boundary:

- Provide a general description of the technical system. Include the primary Hardware and Software (*items listed in table are examples only and should be modified as needed*).

The following system categorization is based on FIPS-199.

Hardware	Purpose
Laptop	Compile and create reports
Firewall	Protect systems from external sources

Software	Purpose
Windows 7	Operating System
Microsoft Office	
McAfee	Anti-virus protection
Adobe Acrobat Reader	Read portable document format (.pdf) files
Java	Mobile code for viewing WWW content
Adobe Flash Player	Multi-media Software

- Include a network diagram that illustrates how the stand-alone systems connect to the Internet and share information.

11. System Configuration Management:

- The Center for Internet Security (CIS) has established benchmarks for various operating systems and tools for assessing these benchmarks. The ISSO will establish minimum baseline requirements with respect to the CIS benchmarks and obtain approval from the ISSM. (*CIS is listed as an example, any baseline standard may be used.*)
- System Updates (identify how HW and SW is updated)
- System Back-ups (describe the system and data back-up procedures)

12. System Interconnections/Information Sharing:

- **Interconnections are not authorized.** Describe how information is shared (e.g., via email, CD/DVD, etc.).

13. Minimum Security Controls:

- The following minimum security controls have been selected for the information systems processing work under contract (*insert contract number*). The contractor will perform a self-assessment on these controls and report to the Contracting Officer’s Representative (COR) and the ISSM.
 1. General Policy Control: This document, and any documents associated with or supportive of this document, is reviewed and updated annually.
 2. Access Control:
 - a. Separate Account Types

- i. Standard user accounts will be used for the routine use of the information systems
 - ii. Administrator accounts will be established for performing tasks requiring elevated privileges (e.g., installing and updating third-party software)
 - b. Establish a policy for disabling accounts upon termination or transfer of personnel that will ensure data integrity
3. Security Awareness & Training:
 - a. All users will take annual security awareness training
 - b. Training records will be maintained
4. Audit & Accountability – not applicable
5. Security Assessment & Authorization:
 - a. The EMCBC will determine security controls
 - b. The EMCBC will evaluate security controls periodically
 - c. The Plan of Action & Milestones (POA&M) will be established to track issues identified as non-compliant with the SSP
6. Configuration Management:
 - a. Apply CIS benchmark recommendations to obtain a minimal score of 80%
 - b. Software must be approved by the Information System Security Officer (ISSO) prior to installation
7. Contingency Planning:
 - a. Establish a methodology for performing data back-ups
 - b. Annually test or validate data back-ups and validate that back-ups are being performed
8. Identification & Authorization:
 - a. Users have unique accounts (shared accounts are not authorized)
 - b. Passwords must be at least 12 characters and meet complexity requirements in accordance with Microsoft's local group policy (upper case letter, lower case letter, special character and number)
 - c. Passwords must be changed every 180 days
 - d. The last 5 passwords cannot be re-used
 - e. Account will be locked out after 5 consecutive invalid logon attempts. Lock-out duration is 15 minutes and the lock-out timer reset is 2 hours.
9. Incident Response:
 - a. Incidents will be reported to the EMCBC Information System Security Manager (ISSM)
10. System Maintenance:
 - a. Maintenance performed by vendors will be approved by the ISSO
11. Media Protection:
 - a. Media will be marked appropriately based on content
12. Physical & Environmental Protection:
 - a. Laptops shall be accounted for and assigned to individuals
 - b. Conduct annual inventory of all equipment
13. Security Planning:
 - a. Establish Rules of Behavior and ensure all users acknowledge
14. Personnel Security:
 - a. Establish personnel sanctions for individuals who violate security policy

- b. No foreign nationals shall be granted access to the system or information without the express written approval of the AODR
15. Risk Assessment:
- a. Review and verify risk categorization annually
 - b. Re-establish configuration benchmarks annually as prescribed in Item 6, Configuration Management
16. System & Services Acquisition:
- a. Obtain documentation for the information system, system component, or information system service that describes secure configuration, installation, and operation of the system, component, or service
17. System & Communication Protection:
- a. System shall be protected by anti-virus software
 - b. System shall be protected by a software firewall (e.g., Microsoft)
 - c. Ensure most recent software patches and updates are installed on the Operating System
 - d. Ensure most recent version of third-party software is installed (e.g., Adobe Flash, Acrobat Reader, McAfee, etc.)
18. System & Information Integrity:
- a. Shall provide for SPAM protection filtering
 - b. Shall provide for malicious code protection through the use of anti-virus software