Compliance Component

Definition

Name	System Security Planning Procedure
Description	The System Security Planning Procedure is a structured process of ensuring adequate security protection of agency systems and information. The outcome of this process is a fully developed System Security Plan that contains technical information about the system, its security requirements and responsibilities, and the controls implemented to provide protection against risks and vulnerabilities.
Rationale	Security of information technology resources is a fundamental management responsibility. Development of System Security Plans improves protection of information technology resources. Such a plan provides a basic overview of the security requirements of the system, security controls, and delineates the responsibilities and expected behavior of those who access the system.
Benefits	• Ensures all elements are considered when planning system security. • Ensures that security is included in the initial and ongoing design of systems.

Associated Architecture Levels

Specify the Domain Name	Security
Specify the Discipline Name	Management Controls
Specify the Technology Area Name	System Security Planning

Compliance Component Type

Document the Compliance Component Type	Guideline

Compliance Detail

State the Guideline, Standard or Legislation	The system security plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Each essential system requires that a System Security Plan be created. A System Security Plan template is available which follows the procedures below (See System Security Plan Template NIST SP 800-18, Appendix A). An essential system or application, for the purposes of this document, typically has most of the characteristics noted below: • Performs clearly defined functions for which there are readily identifiable security considerations and needs • Special considerations are needed based on the criticality of the application or the sensitivity of information contained in, processed, transmitted or stored by the system. • There is potential impact to the agency should there be a security breach (i.e., loss of confidentiality, integrity, or availability). NOTE: The same security plan may apply to many similar systems. For example, each individual workstation could be covered under a comprehensive Security Plan that addresses the use of similar devices.

The System Security plan must address, at a minimum, the following:

System identification, which includes the following:

- Responsible Agency
- System owner(s), administrator(s), security agent(s)
- System name or title
- Brief description of the system
- System environment
- Special considerations
- Interconnections with other systems
- Roles and responsibilities of those who have access to the system

Sensitivity of information, which addresses the following:

- Applicable laws or regulations affecting the system
- General description of the type of information handled by the system and the need for protective measures
- Description of the information's sensitivity, which is determined by requirements for:

  Confidentiality – system contains information that requires protection from unauthorized disclosure

  Integrity – system contains information that must be protected from unauthorized, unanticipated or unintentional modification

  Availability - system contains information or provides services that must be available on a timely basis to meet system requirements or to avoid substantial losses
- Information handling and dissemination rules

Security measures and controls, which includes:

- Security measures, in place or planned, intended to meet the protection requirements of the system.
- Controls (management, operational, and technical) which address:

  Protection requirements to control the security risks

  Security control descriptions indicating whether each is in place or planned

  Hardware and software controls used to provide protection from unauthorized access or misuse

When developing the System Security Plan, the life cycle of the system must be considered.

The system must also undergo periodic risk assessments to identify system vulnerabilities (see the Risk Assessment CC).

Based on the results of a risk assessment, the documented System Security Plan must be updated with any changes needed.

	If the System Security Plan introduces new security issues, considerations may be needed for inclusion of such issues in the agency's security awareness and training program. This document shall be reviewed annually or as needed.
Document Source Reference #	NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems* www.csrc.nist.gov/publications/nistpubs

Compliance Sources

Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name		*Website*	
Contact Information			

Keywords

List Keywords	Systems analysis, identification, classification, planning, permissions, access, vulnerabilities, controls, risk assessment, application development, system lifecycle, template.

Component Classification

Provide the Classification	□ *Emerging*	☒ *Current*	□ *Twilight*	□ *Sunset*
Sunset Date				

Component Sub-Classification

Sub-Classification	Date	Additional Sub-Classification Information
□ *Technology Watch*		
□ *Variance*		
□ *Conditional Use*		

Rationale for Component Classification

Document the Rationale for Component Classification	

Migration Strategy

Document the Migration Strategy	

Impact Position Statement

Document the Position Statement on Impact	

Current Status

Provide the Current Status	□ *In Development*	☒ *Under Review*	□ *Approved*	□ *Rejected*

Audit Trail

Creation Date	03/01/2007	*Date Approved / Rejected*	02/13/2025

Reason for Rejection			
Last Date Reviewed	01/28/2025	*Last Date Updated*	02/13/2025
Reason for Update	Vitality		