Compliance Component

DEFINITION	
Name	Information Security Policy
Description	Information Security Policy is defined as an aggregate of directives, regulations, rules, and practices as approved by senior management that prescribes how an organization manages, protects, and distributes agency information.
Rationale	To provide support and direction from management for information security.
Benefits	• Enhances the agency's overall security posture. • Better prepares the agency for audit and compliance requirements.

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Management Controls
Specify the Technology Area Name	Information Security Policy

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	

State the Guideline, Standard or Legislation	An Information Security Policy document must be approved by management, published and communicated in a form that is relevant, accessible and understandable to the intended reader. It should state management's commitment and establish the agency's approach to managing information security.
	
	At a minimum, the following guidance must be included:
	• A statement of management's intent, which supports the goals and principles of information security.
	• A definition of information security, overall objectives and scope, and the importance of security as an enabling mechanism for information sharing.
	• A brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the agency, for example:
	  ○ Compliance with legislative and contractual requirements
	  ○ Security education requirements
	  ○ Prevention and detection of malicious software
	  ○ Business continuity management
	  ○ Consequences of security policy violations
	• The general and specific responsibilities of agency personnel with regards to information security management, including reporting security incidents

	• References to documentation which support the policy, such as detailed security procedures for specific information systems or security rules. This policy must have an owner who is responsible for its maintenance and review according to a defined review process. That process must ensure that a review takes place in response to any significant changes, such as: • Security incidents • Newly discovered vulnerabilities • Changes to the organizational or technical infrastructure There should also be scheduled, periodic reviews of the following: • The policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents and compliance with industry security standards. • Cost and impact of controls on business efficiency • Effects of changes to technology Agencies should have the following three different types of policies: Program, Issue-Specific and System-Specific **Program** policies should: • Create and define a computer security program. • Be clear as to which resources are covered, including facilities, hardware, software, information, and personnel. • Set agency strategic directions, which include defining the goals of the program. For instance, in an agency responsible for maintaining large mission critical databases, reduction in errors, unauthorized access, data loss, data corruption, and system/data recovery would be specifically stressed. • Assign responsibility for implementing the security program. In most agencies, this will be assigned to security personnel. • Address compliance issues, including detailing responsibilities and establishing specified penalties and disciplinary actions. **Issue-Specific** policies should: • Address specific topics of current relevance and concern to the agency. Management may find it appropriate, for example, to issue a policy on how the agency will approach e-mail privacy or Internet connectivity. • Be updated as needed, such as to keep up with the appropriate use of cutting-edge technology whose security vulnerabilities are still largely unknown. • Contain an issue statement/purpose clause, which includes the agency's position statement, applicability, roles and responsibilities, compliance, and point of contact. **System-Specific** policies should:

	• Focus on decisions taken by agency management to protect a particular system, such as acceptable use of workstations, defining the extent to which individuals will be held accountable for their actions on the system. • Vary from system to system. Each system should have defined security objectives based on the system's operational requirements, environment, and the agency management's acceptance of risk. • Be expressed as rules: who (by job category, organizational placement, or name) can do what (e.g., modify, delete) to which specific classes and records of data, and under what conditions. All three types of policy should be: • Supplemented. Standards, guidelines, and procedures offer users, managers, and others a clearer approach to implementing policy and meeting agency goals. • Visible. Visibility aids implementation of policy by helping to ensure policy is fully communicated throughout the agency. Standards, guidelines, and procedures should be disseminated throughout an agency via handbooks, regulations, or manuals (paper or electronic). • Supported by Management. Without management support, any policy will become ineffective. • Consistent. Other directives, laws, organizational culture, guidelines, procedures, and agency's mission should be considered. This document shall be reviewed annually or as needed.
Document Source Reference #	NIST SP 800-12 Rev.1, An Introduction to Information Security (June 2017)

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

KEYWORDS	
List Keywords	Management directives, management practices, management principles, security rules, program policies, issue policies, system policies, compliance, risk assessment.

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*
Sunset Date				

CURRENT STATUS				
Provide the Current Status	☐ *In Development*	☒ *Under Review*	☐ *Approved*	☐ *Rejected*

AUDIT TRAIL			
Creation Date	2/22/2007	*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		