



Compliance Component

DEFINITION

<i>Name</i>	Information Security Policy
<i>Description</i>	Information Security Policies are senior management's directives for an information security program, to establish its goals, and assign responsibilities.
<i>Rationale</i>	To provide support and direction from management for information security.
<i>Benefits</i>	<ul style="list-style-type: none"> • Provides a common basis for establishing successive information security policies • Provides for effective information security management practices

ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Management Controls
<i>List the Technology Area Name</i>	Information Security Policy
<i>List Product Component Name</i>	

COMPLIANCE COMPONENT TYPE

<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	

COMPLIANCE DETAIL

<i>State the Guideline, Standard or Legislation</i>	<p>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.</p> <p>As a minimum, the following guidance must be included:</p> <ul style="list-style-type: none"> • A definition of information security, overall objectives and scope, and the importance of security as an enabling mechanism for information sharing • A statement of management's intent, which supports the goals and principles of information security • A brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the agency, for example: <ul style="list-style-type: none"> ○ Compliance with legislative and contractual requirements ○ Security education requirements ○ Prevention and detection of viruses and other malicious software ○ Business continuity management
---	---

- Consequences of security policy violations

- A definition of general and specific responsibilities for 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

The 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 changes affecting the basis of the original risk assessment, such as:

- Significant security incidents
- New 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
- 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, data loss, data corruption, and recovery might be specifically stressed.
- Assign responsibility for implementing the security program. In most agencies, this will be assigned to the computer security group.
- 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.

	<ul style="list-style-type: none"> • 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. <p>System-Specific policies should:</p> <ul style="list-style-type: none"> • 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. <p>All three types of policy should be:</p> <ul style="list-style-type: none"> • Supplemented. Standards, guidelines, and procedures offer users, managers, and others a clearer approach to implementing policy and meeting agency goals. Standards, guidelines, and procedures must be disseminated throughout an agency via handbooks, regulations, or manuals (paper or electronic). • Visible. Visibility aids implementation of policy by helping to ensure policy is fully communicated throughout the agency. • Supported by Management. Without management support, the policy will become an empty token of management's "commitment" to security. • Consistent. Other directives, laws, organizational culture, guidelines, procedures, and agency's mission should be considered.
<i>Document Source Reference #</i>	NIST (SP) 800-14 Generally Accepted Principles and Practices for Securing Information Technology, SANS Institute 2003
Standard Organization	
<i>Name</i>	ISO 17799 2000(E) <i>Website</i>
<i>Contact Information</i>	

Government Body			
<i>Name</i>	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	<i>Website</i>	
<i>Contact Information</i>	inquiries@nist.gov		
KEYWORDS			
<i>List all Keywords</i>	Management directives, management practices, management principles, security rules, program policies, issue policies, system policies, compliance, risk assessment.		
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>		
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>			
Conditional Use Restrictions			
<i>Document the Conditional Use Restrictions</i>			
Migration Strategy			
<i>Document the Migration Strategy</i>			
Impact Position Statement			
<i>Document the Position Statement on Impact</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i> <input type="checkbox"/> <i>Under Review</i> <input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>		
AUDIT TRAIL			
<i>Creation Date</i>	2/22/2007	<i>Date Accepted / Rejected</i>	03/23/2007
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			