COMPLIANCE COMPONENT

DEFINITION

Name	Minimum System Security Documentation
Description	Minimum System Security Documentation contains the system life cycle and descriptions of the system hardware, software, policies, standards, procedures, and approvals related to information systems.
Rationale	The documentation of hardware, software, policies, standards, and procedures provide the basis for protecting the integrity, availability, and confidentiality of each of an agency's IT resources. This documentation explains how software and hardware is to be used and serves to formalize the security and operational controls specific to agency's systems.
Benefits	• The availability of formal resource security documentation will aid in ensuring that each systems operational activities are understood • Formalized documentation of operational practices and procedures helps to eliminate security lapses and oversights

ASSOCIATED ARCHITECTURE LEVELS

Specify the Domain Name	Security
Specify the Discipline Name	Operational Controls
Specify the Technology Area Name	Security Documentation
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	• System owners (agencies) must ensure that security documentation exists to provide a reference to how IT resources have been protected.
	
	• The following, minimum documentation, should be current for all resources:
	   o System Security Plan (see System Security Planning CC)
	   o Contingency Plan (see Contingency Plan Development, Documentation and Technical Considerations CC)
	   o Risk Assessment (see Risk Assessment CC)
	   o Acceptable Use policy
	   o Security Certification and Accreditation documents that authorize the system to operate (see Security Certification and Accreditation Process CC)
	   o Standard Operating Procedures
	   o Configuration or Change Management Plans
	
	• The system owner or other IT personnel must maintain supporting system documentation, which may include:
	   o Vendor-supplied software documentation

	o Vendor-supplied hardware documentation
	o Documentation for in-house applications
	o Detailed documentation on operation of networks, routers, and switches if applicable
	o Software and hardware acceptance testing procedures and results
	o Operator's manuals
	• System Security Documentation
	o Is considered a sensitive document and must be protected accordingly
	o Must include change management
	o Must be kept current during the entire system lifecycle
Document Source Reference #	NIST SP 800-18, Guide for Developing Security Plans for Information Technology 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	Integrity, availability, confidentiality, backup, contingency, procedure, policies, guideline, standard, change management, IT resources.

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*	03/23/2007
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			