COMPLIANCE COMPONENT

DEFINITION	
Name	Agency Security Roles and Responsibilities
Description	Agency Security Roles and Responsibilities define the requirement(s) of agency officials who must be involved in information security.
Rationale	In order for an information security program to be effective there must be clear lines of responsibility and accountability. These responsibilities should be handled in a manner appropriate for the agency. While it is important that there be clear lines of responsibility and accountability, ultimately information security is "everyone's" duty.
Benefits	• Clarifies the important roles and responsibilities of agency management and staff at all levels with regards to information security.

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Management Controls
Specify the Technology Area Name	Personnel Security
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	There are specific roles necessary to administer information security. The following are principle agency roles and associated responsibilities in information security. • Senior Agency Management o Establishes the agency's information security policy and its overall program goals, objectives, and priorities in order to support the mission of the agency. Ultimately, the head of the agency is responsible for ensuring that adequate resources are applied to the security program and that it is successful. • Information Security Management o Includes the Chief Information Security Officer and support staff, which directs the agency's day-to-day management of its information security program. The Chief Information Security Officer is also responsible for coordinating all security-related interactions among those impacted by the information security program. • Agency Functional Managers and Information Owners o Responsible for a systems or functions documentation and providing input on management, operational, and technical controls. Technology Providers • System Management or System Administrators

	o Managers and technicians who design and operate information technology systems. They are responsible for implementing technical security and for being familiar with security technology that relates to their system. They also need to ensure the continuity of their services to meet the needs of functional managers, analyzing technical vulnerabilities in their systems, and maintaining system documentation. • Office of Cyber Security o Responsible for the day-to-day security implementation, documentation and policy administration of information technology systems. • End User Support and Help Desk o Documents and informs the Office of Cyber Security of suspicious activity.
Document Source Reference #	NIST SP 800-12 Rev. 1, An Introduction to Information Technology Security: The NIST Handbook

Compliance Sources			
Name	National Institute of Standards and Technology (NIST), Information Technology Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		
Name	NIST SP800-12 Rev. 1 An Introduction to Computer Security: The NIST Handbook.	*Website*	https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final
Contact Information	inquiries@nist.gov		

KEYWORDS	
List Keywords	administration, policy, procedures, planning, staffing, roles, responsibilities, controls

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	02/09/06	*Date Approved / Rejected*	06/14/2018
Reason for Rejection			
Last Date Reviewed	06/14/2018	*Last Date Updated*	06/14/2018
Reason for Update	Vitality		