COMPLIANCE COMPONENT

DEFINITION	
Name	Separation of duties
Description	Separation of duties divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud.
Rationale	Provides process integrity while maintaining proper security and quality controls.

Benefits	• Having different staff engaged within an end-to-end process is a common, sensible business practice that ensures consistent and successful execution of the process.
	• No one person has control over the lifespan of a transaction.
	• Effective separation of duties provides for a system of checks and balances when following the general principles below:
	  • Separate system ownership from the system certification/accreditation process
	  • Separate system administration from system auditing.
	  • Separate operational responsibility from record keeping responsibility
	
	NOTE: Adhering to these principles may not be possible due to resource limitations or other considerations. In these cases, the risk resulting from inadequate separation of duties should be assessed to ensure that the level of exposure is acceptable to an agency or division management.

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	Separation of duties must be established and documented to ensure individuals do not have access to more than one critical task, as identified by management.
	Examples of tasks that should be performed by different individuals:
	  ○ Development
	  ○ Testing
	  ○ Administration (e.g. database, systems, network, etc.)
	  ○ Physical security
	  ○ IT security

	An audit policy should be established to ensure compliance with the separation of duties policy.		
Document Source Reference #	NIST SP 800-12 Rev. 1, An Introduction to Computer Security (June 2017)		
Compliance Sources			
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			
Name		*Website*	
Contact Information			
Name		*Website*	
Contact Information			
KEYWORDS			
List Keywords	Management, administration, policy, procedures, planning, staffing, critical tasks, sensitive, data.		
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	05/25/06	*Date Approved / Rejected*	05/16/2019
Reason for Rejection			
Last Date Reviewed	05/09/2019	*Last Date Updated*	05/09/2019
Reason for Update			