COMPLIANCE COMPONENT

DEFINITION

Name	Separation of Duties
Description	Separation of Duties refers to dividing roles and responsibilities to minimize the possibility that a single individual can cause a security breach.
Rationale	Establishes division of responsibilities and separates duties of individuals as necessary to minimize security-related risk.
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. • Separation of duties helps to reduce fraud and malicious damage, because any user attempting to engage in such activities would be forced to collude with at least one other user. • Separation of duties also reduces errors, because a second operator will often catch mistakes made or missed by the first. NOTE: In situations where the agency cannot support the differentiation of roles or a single individual performs all roles within the agency, the agency shall employ appropriate compensating controls (e.g., providing increased personnel security and auditing measures).

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	The general principle of the control is that malicious collusion between two or more authorized individuals is much less likely than one person engaging alone in inappropriate behavior. Separation of duties minimizes the ability of individuals from having the information system access necessary to perform malicious activity without collusion. Examples of separation of duties include: • Agency critical functions are divided among different individuals or roles.

	• Distinct information system support functions and mission critical functions are divided among different individuals or roles.
	
	• Different individuals perform information system functions, examples:
	    o Development
	    o Testing
	    o Administration (e.g. database, systems, network, etc.)
	    o Physical security
	    o IT Security
	    o Provisioning

Document Source Reference #	NIST Special Publications: 800-53 Rev. 5 and 800-12 Rev. 1

Compliance Sources		
Name	NIST SP800-53 Rev. 5 - Recommended Security Controls for Federal Information Systems and Organizations	*Website*	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
Contact Information		
Name	NIST SP800-12 Rev. 1 An Introduction to Computer Security: The NIST Handbook.	*Website*	*An Introduction to Information Security (nist.gov)*
Contact Information		

KEYWORDS	
List Keywords	Management, administration, policy, procedures, planning, staffing, critical tasks, sensitive, data, collusion, responsibility, duties, fraud, data breach

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*	06/13/06
Reason for Rejection			
Last Date Reviewed	03/14/2023	*Last Date Updated*	03/16/2023
Reason for Update	Vitality		