COMPLIANCE COMPONENT

DEFINITION	
Name	User Authorization
Description	User Authorization is the use of access control policies and associated access enforcement mechanisms that are employed by agencies to control access between users and objects.
Rationale	User authorization is used to mitigate risk to agency operations, assets, and individuals associated with information access.
Benefits	• Helps protect agency resources and information • Allow users access to only those resources needed (least privilege) • Protects users from accidentally accessing unneeded resources and information

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Technical Controls
Specify the Technology Area Name	Identification and Authorization
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	User Authorization should be based on least privilege • The information system enforces the most restrictive set of rights and privileges or accesses needed by users • Processes acting on behalf of users for the performance of specified tasks o Including specific ports, protocols, and services • The agency employs the practice of least privilege for specific duties and information systems in accordance with risk assessments User Authorization access control policies should require • Documented procedures which facilitate the implementation of the access control policy and associated access controls o Address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance • Developed, disseminated, and periodically reviewed policies and associated access enforcement mechanisms • Access to the information system based on: o A valid need-to-know that is determined by assigned duties

	o Intended system usage • Access administrators are notified when system users are: o Terminated o Transferred o Assigned to different tasks Additional Access Controls • In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the agency. • In the event of emergencies or other serious events, consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms. Information Flow Control • The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. • Flow control is based on the characteristics of the information. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Separation of Duties • The information system enforces separation of duties through assigned access authorizations. (See Separation of Duties CC).
Document Source Reference #	NIST SP 800-53

Compliance Sources

Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information			
Name		*Website*	
Contact Information			

KEYWORDS

List Keywords	Control, access, need-to-know, separation of duties, information flow, least privilege.

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	01/04/2007	*Date Approved / Rejected*	03/23/2007
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			