COMPLIANCE COMPONENT

DEFINITION	
Name	Access Controls
Description	Access Controls prescribe who or what is to have access to a specific system resource and the type of access permitted.
Rationale	Access controls allow (or prohibit) the use of various computer resources. Users must have access to the resources they need to perform their job duties, but no more. Access controls enforce policy and help ensure that unauthorized actions are not permitted.
Benefits	Access controls: ▪ Prescribe who or what is to have access to a specific system resource ▪ Prescribe type of access that is permitted ▪ Protect operating systems and other system software from unauthorized modification or manipulation ▪ Protect the integrity and availability of information by restricting the number of users and processes with access ▪ Helps protect confidential information from being disclosed to unauthorized individuals

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Technical Controls
Specify the Technology Area Name	Logical Access Controls
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 requirements for using—and prohibitions against the use of—various system resources vary considerably from one system to another. Access is based on the concept of least privilege. It may also be important to control the kind of access that is permitted (e.g., the ability for the average user to execute, but not change, system programs). These types of access restrictions enforce policy and help ensure that unauthorized actions are not taken. Access control is the process of granting or denying specific requests to: 1) Obtain and use information and related information processing services 2) Enter specific physical facilities (e.g., state buildings, data centers, correctional facilities, state hospitals). System-based access controls are called logical access controls. **Logical access controls** can prescribe not only who or what (in the case of a process) is to have

	access to a specific system resource, but also the type of access that is permitted. These controls may be built into the operating system, incorporated into applications programs or major utilities (e.g., database management systems, communications systems), or implemented through add-on security packages. Logical access controls may be implemented internally to the system being protected or in external devices. Examples of access control security controls include: • account management • separation of duties • least privilege • session lock • information flow enforcement • session termination Organizations limit: 1) System access to authorized users 2) Processes acting on behalf of authorized users 3) Devices, including other systems 4) Types of transactions and functions that authorized users are permitted to exercise This document will be updated annually.
Document Source Reference #	NIST SP 800-12 Rev. 1, Guide to Computer Security (June 2017)

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	logical, physical, password, database, protection, access.

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	02/01/2007	*Date Approved / Rejected*	03/23/2007
Reason for Rejection			
Last Date Reviewed	03/14/2023	*Last Date Updated*	03/16/2023
Reason for Update	Vitality		