



COMPLIANCE COMPONENT

DEFINITION	
<i>Name</i>	Maintaining User Accounts
<i>Description</i>	Maintaining User Accounts involves the process of requesting, establishing, issuing, modifying, and terminating user accounts along with tracking user access authorizations.
<i>Rationale</i>	Maintaining User Accounts reinforces individual accountability and helps keep information secure by granting the user the least amount of permission necessary to accomplish their job functions.
<i>Benefits</i>	<ul style="list-style-type: none"> • No idle accounts are available, limiting possible security vulnerabilities. • Users only have permissions necessary to perform their current job functions. • Provides methodology for auditing user accounts.
ASSOCIATED ARCHITECTURE LEVELS	
<i>Specify the Domain Name</i>	Security
<i>Specify the Discipline Name</i>	Operational Controls
<i>Specify the Technology Area Name</i>	Personnel Security
<i>Specify the Product Component Name</i>	
COMPLIANCE COMPONENT TYPE	
<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	
COMPLIANCE DETAIL	
<i>State the Guideline, Standard or Legislation</i>	<p>Usernames</p> <ul style="list-style-type: none"> • Usernames must be unique and must follow a standard naming convention. Naming conventions should take several factors into account: <ul style="list-style-type: none"> ○ The chance of duplicate usernames ○ The structure of your agency ○ The constraints of the applications ○ The confidentiality of the username (for example, not using the SSN) ○ The change of a username. Such changes must consider: <ul style="list-style-type: none"> ▪ All affected systems ▪ Updating the ownership of all files and other user-specific resources ▪ Handling email issues ▪ Removal of previous username from affected systems

	<ul style="list-style-type: none"> • A username must identify a unique individual or resource at any given time if the username has permission to make modifications to systems or information <p>Authentication</p> <ul style="list-style-type: none"> • See the Password Controls CC and the Strong Authentication CC <p>Access Control Information</p> <ul style="list-style-type: none"> • See the Logical Access Controls TA. • A user account must be appropriately reconfigured to add or remove accesses after a job change • Agencies must have a procedure where the IT department is notified in a timely manner of a new person's arrival and the accesses required • Agencies must have a procedure where the IT department is notified in a timely manner of a person's departure. At the very least, the appropriate actions should include: <ul style="list-style-type: none"> ○ Immediately disabling the user's access to all systems and related resources ○ Preserving the user's files to meet compliance standards in case something is needed at a later time ○ Coordinating access to the user's files with the user's manager <p>Audit and Management Reviews</p> <ul style="list-style-type: none"> • Agencies must periodically review user accounts, to include at least the following: <ul style="list-style-type: none"> ○ Levels of authorized access for each user ○ Identification of inactive, idle or orphaned accounts ○ Whether required training or certification has been completed • These reviews can be conducted on at least two levels <ul style="list-style-type: none"> ○ On an application-by-application basis ○ On a system wide basis • Both levels of reviews can be conducted by <ul style="list-style-type: none"> ○ In-house systems personnel (a self-audit) ○ The agency's internal audit staff ○ External auditors 		
<i>Document Source Reference #</i>	NIST Special Publication 800-12 Rev. 1, An Introduction to Computer Security		
Compliance Sources			
<i>Name</i>	NIST	<i>Website</i>	csrc.nist.gov
<i>Contact Information</i>	inquiries@nist.gov		
<i>Name</i>		<i>Website</i>	

<i>Contact Information</i>			
KEYWORDS			
<i>List Keywords</i>		Audit, user ID, username, account name, password, authentication, access control, authorization, permissions, tracking, active directory, RACF, AD, idle, orphaned, inactive, web application	
COMPONENT CLASSIFICATION			
<i>Provide the Classification</i>		<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>	
<i>Sunset Date</i>			
COMPONENT SUB-CLASSIFICATION			
<i>Sub-Classification</i>	<i>Date</i>	<i>Additional Sub-Classification Information</i>	
<input type="checkbox"/> <i>Technology Watch</i>			
<input type="checkbox"/> <i>Variance</i>			
<input type="checkbox"/> <i>Conditional Use</i>			
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>			
Migration Strategy			
<i>Document the Migration Strategy</i>			
Impact Position Statement			
<i>Document the Position Statement on Impact</i>			
CURRENT STATUS			
<i>Provide the Current Status</i>		<input type="checkbox"/> <i>In Development</i> <input type="checkbox"/> <i>Under Review</i> <input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>	
AUDIT TRAIL			
<i>Creation Date</i>	03/02/2006	<i>Date Approved / Rejected</i>	02/07/2023
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>	02/01/2023	<i>Last Date Updated</i>	02/10/2023
<i>Reason for Update</i>	Vitality		