



Compliance Component

DEFINITION

<i>Name</i>	Maintaining User Accounts
<i>Description</i>	<p>Maintaining User Accounts involves the process of requesting, establishing, issuing, and closing user accounts along with tracking user access authorizations and managing these functions.</p> <p>A user account is composed of the username, an authentication mechanism such as a password (see the Password Controls CC), and access control information (see the Logical Access Controls TA).</p>
<i>Rationale</i>	Maintaining User Accounts is a continuing process. New user accounts are added while others are deleted. Permissions can change. New applications are added, upgraded, and removed. Tracking this information to keep it up-to-date is necessary to allow users' access to only those functions necessary to accomplish their assigned responsibilities, thereby helping to maintain the principle of least privilege.
<i>Benefits</i>	<ul style="list-style-type: none"> • No idle accounts are available to hackers • Users only have permissions necessary to perform their current jobs • New users obtain unique identifiers in a timely manner • Provides methodology for the audit logs to be effective

ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Management Controls
<i>List the Technology Area Name</i>	Personnel Security
<i>List 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>Username</p> <ul style="list-style-type: none"> • Usernames must be unique and must follow a 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 organization
---	--

- The constraints of the applications
- The confidentiality of the username (for example, not using the SSN)
- The chance that appending different data together to form a username creates the potential for the result being inappropriate
 - A review process should be in place before finalizing a username
- The change of a username. Such changes must consider:
 - Necessary changes to all affected systems
 - Keeping the underlying user identification constant
 - Changing the ownership of all files and other user-specific resources
 - Handling email issues
- 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.

Authentication

- See the Password Controls CC and the Strong Authentication CC.

Access Control Information

- 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:
 - Immediately disabling the user's access to all systems and related resources
 - Backing up the user's files in case something is needed at a later time
 - Coordinating access to the user's files with the user's manager

Audit and Management Reviews

- Agencies must periodically review user accounts, to include at least the following:
 - 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
 - On an application-by-application basis
 - On a system wide basis.

	<ul style="list-style-type: none"> Both kinds 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, An Introduction to Computer Security		
Standard Organization			
<i>Name</i>	NIST, CERT® Coordination Center	<i>Website</i>	csrc.nist.gov, www.cert.org
<i>Contact Information</i>			
Government Body			
<i>Name</i>		<i>Website</i>	
<i>Contact Information</i>			
KEYWORDS			
<i>List all Keywords</i>	Audit, user ID, user name, account name, password, authentication, access control, authorization, permissions, tracking, active directory, RACF, ADS, idle, orphaned, inactive		
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>		
Rationale for Component Classification			
<i>Document the Rationale for Component Classification</i>			
Conditional Use Restrictions			
<i>Document the Conditional Use Restrictions</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 Accepted / Rejected</i>	06/13/06
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			