Compliance Component

Definition

Name	Maintaining User Accounts
Description	Maintaining User Accounts involves the process of requesting, establishing, issuing, modifying, and terminating user accounts along with tracking user access authorizations.
Rationale	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.
Benefits	• 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

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

<table>
<tr>
<td><i>State the Guideline, Standard or Legislation</i></td>
<td>
<b>Usernames</b>
<ul>
<li>Usernames must be unique and must follow a standard naming convention. Naming conventions should take several factors into account:
<ul>
<li>The chance of duplicate usernames</li>
<li>The structure of your agency</li>
<li>The constraints of the applications</li>
<li>The confidentiality of the username (for example, not using the SSN)</li>
<li>The change of a username. Such changes must consider:
<ul>
<li>All affected systems</li>
<li>Updating the ownership of all files and other user-specific resources</li>
<li>Handling email issues</li>
<li>Removal of previous username from affected systems</li>
</ul>
</li>
</ul>
</li>
</ul>
</td>
</tr>
</table>

- 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
  - 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

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
- Both levels of reviews can be conducted by
  - In-house systems personnel (a self-audit)
  - The agency’s internal audit staff
  - External auditors

This document will be reviewed annually or as needed.

Document Source Reference #	NIST Special Publication 800-12 Rev. 1, An Introduction to Computer Security		
Compliance Sources			
Name	NIST	*Website*	csrc.nist.gov
Contact Information	inquiries@nist.gov		
Name		*Website*	

Contact Information	

KEYWORDS

List Keywords	Audit, user ID, username, account name, password, authentication, access control, authorization, permissions, tracking, active directory, RACF, AD, idle, orphaned, inactive, web application

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	03/02/2006	***Date Approved*** */ Rejected*	02/19/2025
Reason for Rejection			
Last Date Reviewed	02/19/2025	*Last Date Updated*	02/19/2025
Reason for Update	Vitality		