

***{SYSTEM NAME}***

**Identity and Access Management SOP**

**Version x**

**Approval Date:**

**mm/dd/yyyy**

**{SYSTEM NAME} Identity and Access Management SOP**

This document captures the minimum requirements.

|  |  |  |
| --- | --- | --- |
| **Version Number** | **Date** | **Description** |
| **x.x** | **mm/dd/yyyy** | **Initial Document** |
|  |  |  |
|  |  |  |
|  |  |  |

**Table of Contents**

[1.0 Purpose 1](#_Toc508549469)

[2.0 Scope 1](#_Toc508549470)

[3.0 Types of Users 1](#_Toc508549471)

[4.0 Password Policy and Procedures (AC-1) 2](#_Toc508549472)

[4.1 Shared Accounts (IA-2) 2](#_Toc508549473)

[4.2 Primary (End User) Passwords (IA-5(1)) 3](#_Toc508549474)

[4.3 Secondary (Privileged) Accounts (IA-5(1)) 3](#_Toc508549475)

[4.4 Procedures for changing/resetting passwords (IA-5(1)) 4](#_Toc508549476)

[4.5 Forgotten or Compromised Passwords (IA-5(1)) 5](#_Toc508549477)

[4.6 Caching (Embedding) Passwords (IA-5(7)) 5](#_Toc508549478)

[4.7 Separation of Duties and Least Privilege (AC-5, AC-6 (Moderate only)) 5](#_Toc508549479)

[4.8 Authenticator Feedback (IA-6) 6](#_Toc508549480)

[4.9 Unsuccessful Login Attempts (AC-7) 6](#_Toc508549481)

[4.10 Session Lock/System Inactivity (AC-11, AC-11(1) (Moderate Only), and AC-12) 7](#_Toc508549482)

[5.0 Account Lifecycle Policy and Procedures (IA-1) 7](#_Toc508549483)

[5.1 Device Identification and Authentication (IA-3 and AC-4) 7](#_Toc508549484)

[5.2 Identifier Management (IA-4) 8](#_Toc508549485)

[5.3 Authenticator Management (IA-5) 8](#_Toc508549486)

[5.4 Account Management (AC-2) 9](#_Toc508549487)

[5.5 System Use Notification (Warning Banners) (AC-8) 9](#_Toc508549488)

[5.6 Permitted Actions without Identification and Authentication (i.e., Public Access) (AC-14) 11](#_Toc508549489)

[5.7 Publicly Accessible Content (AC-22) 11](#_Toc508549490)

**[DELETE THIS PARAGRAPH]** *- This Identity and Access Management template is written for all Low and Moderate System Impact levels as defined in FIPS 199, and is intended only as a sample of one methodology. Areas with a red italics are instructional, and words in* ***blue text*** *are to be replaced with pertinent information (e.g., system name(s), acronym(s), I/C name, organization name, etc.). Areas in Yellow highlights are illustrative and should be replaced with relevant content for your system.*

# Purpose

The purpose of this document is to establish the password policy and standards for the administration of application and user accounts that facilitate access or changes to {SYSTEM NAME}’s information systems and data. A {SYSTEM NAME} account, at a minimum, consists of [example: an NIH approved domain user account; a {SYSTEM NAME} provided user ID and a password, etc.]. Supplying account information to approved administrators and end users will grant specific role based access to some set of services and resources within {SYSTEM NAME}. This document establishes guidelines for issuing accounts, creating password values, and managing accounts throughout the account life cycle.

# Scope

This guide is applicable to those responsible for the management of {SYSTEM NAME} and for managing end user (application) accounts, as well as for any privileged user accounts, if applicable. User account information can be held within a database or directory (i.e., Active Directory, LDAP), within an application, or may be federated or single-sign on solution (i.e., SAML, iTrust/Siteminder, etc.). This document covers all types of {SYSTEM NAME} accounts including privileged (administrator) and end users to the extent they apply. The writer should address those areas of a given control where control falls within the application’s control, and should state where any aspects are inherited from a parent system or organization. For example, if an application leverages NIH Active Directory user IDs, then many aspects related to credential issuance, password management, and account life cycle are inherited. In such cases, this SOP should address where and how the application will use those identifiers in areas like role and privilege management, auditing of user activities in the application, locking the application when excess failed attempts occur, etc.

# Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 3‑1 Personnel Roles and Privileges that follows.

Instruction: For an External User, write “Not Applicable” in the Sensitivity Level Column. This table must include all roles including systems administrators and database administrators as a role types. (Also include web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact the application.)

This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.

Delete this and all other instructions from your final version of this document.

Table 3‑1 Personnel Roles and Privileges

| Role | Internal or External | Privileged (P), Non-Privileged (NP), or No Logical Access (NLA) | Sensitivity Level | Authorized Privileges | Functions Performed |
| --- | --- | --- | --- | --- | --- |
|  | Choose an item. | Choose an item. | Choose an item. | Full administrative access (root) | Briefly explain functions performed |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

# Password Policy and Procedures (AC-1)

## Shared Accounts (IA-2)

*Instruction: Describe the {SYSTEM NAME} policy regarding the use of shared user accounts. Note that per NCI policy, the use of Shared Accounts is PROHIBITED unless operationally necessary. Delete this instruction from the final document version.*

{SYSTEM NAME} adheres to the NCI policy regarding the use of shared user accounts, and applies the following practices and procedures to ensure the policy is met:

* Step 1
* Step 2
* Etc.

NCI Shared Account Policy:

* + *The use of shared accounts is prohibited unless operationally necessary;*
  + *Such exceptions require documentation that justifies the need and a copy of the justification must be available upon request such as during a formal audit or data call.*
  + *Each shared account must have a designated owner, responsible for the management of access to that account;*
  + *The account owner must maintain a list of individuals who have access to the shared account*

## Primary (End User) Passwords (IA-5(1))

*Instruction: Describe the {SYSTEM NAME} End User password policy as it relates to the following NCI policies. (If system provides only anonymous access such as a public information dissemination website, state ‘Not Applicable (N/A)’ for user passwords. Delete this instruction from the final document version*

{SYSTEM NAME} adheres to the NCI password policy, and applies the following practices and procedures to ensure the policy is met:

* Step 1
* Step 2
* Etc.

NCI Password Policy:

*Users must choose passwords that have at least eight characters and satisfy all four of the following conditions:*

* + *Includes at least one capital letter (ABCDEFG…)*
  + *Includes at least one lower case letter (abcdefg…)*
  + *Includes at least one numeric character (012345…)*
  + *Includes at least one special character (*[!@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./)](mailto:!@#$%^&*()_+|~-=\`{}[]:";'<>?,./))

## Secondary (Privileged) Accounts (IA-5(1))

*Describe the {SYSTEM NAME} privileged account password policy as it relates to the following NCI Policies. Delete this instruction from the final document version.*

{SYSTEM NAME} adheres to the NCI privileged/secondary user account policy, and applies the following practices and procedures to ensure the policy is met:

* Step 1
* Step 2
* Etc.

NCI Policy:

*Secondary or Privileged users (system admins, root users, etc.) are responsible for the following:*

* *Using a 15 character passphrase*
* *Password must meet the same complexity rules as end user passwords, including containing all of the following:*

*- At least one capital letter (ABCDEFG…)*

*- At least one lower case letter (abcdefg…)*

*- At least one numeric character (012345…)*

*- At least one special character (*[!@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./)](mailto:!@#$%^&*()_+|~-=\`{}[]:";'<>?,./))

* *Ensuring that password files are not stored or transmitted in plain text to prevent disclosure.*
* *Encrypting passwords using NIST-approved encryption whenever operationally feasible.*
* *Ensuring that the user accounts that have elevated privileges (e.g. admin or dev) granted through group memberships or utilities that allow temporary root access for Systems Administrators have a unique password from all other accounts held by that user.*
* *Changing vendor supplied (default) passwords and accounts immediately.*
* *Not using their Admin or Dev account to access or send e-mail, for web browsing, or any other routine office work.*
* *Only using their Admin or Dev account when required.*

## Procedures for changing/resetting passwords (IA-5(1))

*Describe the {SYSTEM NAME} Password change/reset policy and procedures as it relates to the following NCI Policy. Delete this instruction from the final document version.*

{SYSTEM NAME} adheres to the NCI password lifetime (i.e., change/reset) policy, and applies the following practices and procedures to ensure the policy is met:

* Step 1
* Step 2
* Etc.

NCI Password Lifetime Policy:

* *Users must change passwords at least every 120 days to one that is different from the previous 24 passwords used;*
* *Password length and complexity must meet the policies stated above for either a) Admin or Dev accounts, or b) end user accounts, as appropriate;*
* *When a user’s password is initially set or reset by a system administrator the user must change the temporary password the first time they use it.*
* *Minimum password lifetime is 1 day.*

## Forgotten or Compromised Passwords (IA-5(1))

*Describe the procedures for managing forgotten, lost, or compromised primary (end user) and/or secondary (privileged) account passwords for {SYSTEM NAME}. Delete this instruction from the final document version.*

* Step 1
* Step 2
* Etc.

**{SYSTEM NAME} Lost or Forgotten Password Policy:**

[*SAMPLE TEXT] Compromised passwords (i.e., stolen passwords or suspected compromised passwords) must be reported to the NIH Help Desk at 301-496-4357. The Help Desk will contact NCI. Forgotten Active Directory passwords may be reset by an authorized administrator or by using a self-service website utility. An authorized NIH AD user who has forgotten their password is authorized to use a co-worker’s computer in the presence of the co-worker, provided that co-worker consents and is an AD authorized user, for the sole purpose of accessing NIH password self-service utilities noted in the NIH User Password Guidance.*

## Caching (Embedding) Passwords (IA-5(7))

*Define {SYSTEM NAME} policy (if any) regarding the use of cached/stored passwords (including user, system and resource accounts) as it relates to the following NCI Policy:*

* Step 1
* Step 2
* Etc.

NCI Policy:

*Passwords should not be stored in websites, programs or scripts, if operationally feasible.*

## Separation of Duties and Least Privilege (AC-5, AC-6 (Moderate only))

*Define {SYSTEM NAME} Policies and Procedures regarding the Separation of Duties and Least Privilege as they relate to the following NCI policies:*

* Step 1
* Step 2
* Etc.

[SAMPLE TEXT] *End Users’ and Privileged (i.e., Admin, Developer, etc.)’ access to the {SYSTEM NAME} shall be assigned and restricted based on assigned role or function within the system, and be limited to the minimum level of access necessary to perform the assigned duties within the system. Security related user roles will be divided between different roles (i.e., system administration, development, application administration, configuration management, quality assurance and testing, network security, system and application auditing, etc.) through the use of role based access control (RBAC) to the extent feasible and practicable. Users will be assigned to groups or roles, which have appropriate permissions and privileges pre-assigned to them. Users must be issued and must use only non-privileged (i.e., regular end-user) account credentials when performing non-privileged activities in the system or application.*

NCI Policy:

***AC-5***

*1. Ensure that audit functions are not performed by security personnel responsible for administering access control.*

*2. Maintain a limited group of administrators with access based upon the users' roles and responsibilities.*

*3. Ensure that critical mission functions and information system support functions are divided among separate individuals.*

*4. Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups.*

*5. Ensure that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system****.***

***AC-6 (Moderate Impact Only)***

*1. Disable all file system access not explicitly required for system, application, and administrator functionality.*

*3. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control.*

*4. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties.*

## Authenticator Feedback (IA-6)

* Describe/Confirm that user credentials are not displayed in readable format on-screen while user enters password or other authenticator (e.g., PIN):

*Ensure systems that require interactive user authentication obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals*

## Unsuccessful Login Attempts (AC-7)

*Describe the {SYSTEM NAME} unsuccessful logon settings as it relates to the following NCI policy.*

* Session/System Lockout Settings:

NCI Policy:

*When the system supports it, the maximum number of invalid user logon attempts during a 60 minute window is six (6). The account must then remain locked for at least 30 minutes or until manually reset by an authorized administrator or by using a self-registration/reset utility.*

## Session Lock/System Inactivity (AC-11, AC-11(1) (Moderate Only), and AC-12)

*Describe the {SYSTEM NAME} Policy for managing idle authenticated user sessions as it relates to the following NCI policies.*

* Step 1
* Step 2
* Etc.

NCI Policy:

*AC-11: Session lock mechanisms will be activated for user workstations and server consoles and other systems automatically after 15 minutes or less of inactivity for both remote and internal access connections, when technically and operationally feasible.* ***Users must deliberately log out of their computers or lock their screen when they leave their desks.***

*AC-11(1): The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.*

*AC-12: The information system automatically terminates a user session after [Assignment:*

* *30 minutes of inactivity*
* *NIH Threat Mitigation & Incident Response (TMIR) targeted responses to attacks on NIH networks and resources*
* *Violations of the NIH General Rules of Behavior*
* *Violations of the NIH Mobile Device Rules of Behavior*
* *Violations of the NIH Rules of Behavior for Privileged User Accounts*
* *Deviations from the NIH Anti-Virus Standard*
* *Time-of-day restrictions on information system users or selected user accounts*

# Account Lifecycle Policy and Procedures (IA-1)

Accounts that access {SYSTEM NAME} require vigilant management and supervision. The following security precautions are implemented for account management:

## Device Identification and Authentication (IA-3 and AC-4)

*Describe the process for ensuring that specific devices (e.g., other systems, other networks, etc.) are uniquely identified and authenticated to {SYSTEM NAME}. You may include any or all of the following:*

* *Specific Systems or Devices that are permitted to access/connect to {SYSTEM NAME}*
* *Method by which each system/device are identified (e.g., MAC address, TCP/IP address, TNSNames, etc.)*
* *Method by which each system is authenticated (e.g., IEEE 802.1x, Database file, RADIUS Server with EAP-TLS, Kerberos, etc.)*
* Step 1
* Step 2
* Etc.

## Identifier Management (IA-4)

*Describe the following Identifier Management processes for {SYSTEM NAME}*

*Receiving authorization from defined personnel or roles (defined in the applicable security plan) to assign an individual, group, role, or device identifier;*

*Selecting an identifier that identifies an individual, group, role, or device;*

*Assigning the identifier to the intended individual, group, role, or device;*

*Preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three (3) years has expired; and*

*Disabling the identifier after sixty (60) days or less of inactivity and deleting disabled accounts during the annual re-certification process*

* Step 1
* Step 2
* Etc.

## Authenticator Management (IA-5)

*Describe the following Authenticator Management practices for HCMI Searchable Catalog.*

*Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;*

*Establishing initial authenticator content for authenticators (passwords, tokens, biometrics);*

*Ensuring that authenticators (e.g., passwords, PIV card, other two –factor solution, system IP/MAC address, etc.) have sufficient strength of mechanism for their intended use;*

*Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;*

*Changing default content of authenticators upon information system installation;*

*Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);*

*Changing/refreshing authenticators [Assignment: at the following intervals:*

*• Passwords – no longer than every 60 days, immediately in the event of known or suspected compromise, and immediately upon system installation (e.g. default or vendor-supplied passwords)*

*• PIV Compliant Access Cards – no longer than every five (5) years*

*• PKI certificates issued in accordance with Federal PKI Common Policy – no longer than every three (3) years*

*Note: For High Value Assets, the organization changes/ refreshes authenticators at least annually for cryptographic devices; and changes/refreshes authenticators at least annually or upon departure of key personnel with knowledge of password for service and system account passwords/pins.;*

*Protecting authenticator content from unauthorized disclosure and modification; and*

*Requiring users to take, and having devices implement, specific measures to safeguard authenticators.*

*Changing authenticators for group/role accounts when membership to those accounts changes.*

*Any PKI authentication request must be validated by Online Certificate Status Protocol (OCSP) or certificate revocation list (CRL) to ensure that the certificate being used for authentication has not been revoked.*

* Step 1
* Step 2
* Etc.

## Account Management (AC-2)

*Describe the processes used to address/implement the following account management controls and control enhancements for {SYSTEM NAME}:*

*Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);*

*Establishing conditions for group membership;*

*Identifying authorized users of the information system and specifying access privileges;*

*Requiring appropriate approvals for requests to establish accounts;*

*Establishing, activating, modifying, disabling, and removing accounts;*

*Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;*

*Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;*

*Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;*

*Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and*

*Reviewing accounts at least annually to ensure unused and un-needed accounts are properly disabled, removed, or archived.*

NCI Moderate Enhancement Policies:

In addition to the above, **Moderate Impact** systems must employ the following enhancements, or compensating control(s) when not possible:

* The organization employs automated mechanisms to support the management of information system accounts.
* The information system automatically terminates temporary and emergency accounts after [Assignment: Temporary (Low=365 days, Mod=60 days or less) Emergency Accounts (Low=180 days, Mod=60 days or less.)]
* The information system automatically disables inactive accounts after [NIH Policy: no longer than 60 days since last successful login].
* The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.
* Step 1
* Step 2
* Etc.

## System Use Notification (Warning Banners) (AC-8)

*Describe the system use notification and procedures for {SYSTEM NAME}:*

*NIST requires that the following are addressed:*

*a. [System] displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording;*

*b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and*

*c. For publicly accessible systems: (i) displays the system use information (banner) when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.*

HHS/NIH Policy:

*Warning banners must be posted at all NIH logon points. Where feasible, the banner should be interactive (pre-login), requiring users to click a button to accept the conditions.*

*The approved HHS warning banner language is below. Institutes and Centers (ICs) can add to the banner provided the additional language does not imply any level of privacy being given to the users, but cannot remove any of the approved language. NIH has approved the following system use notices to be used for all I/Cs:*

The following System Use Notice(s) are posted for the {SYSTEM NAME}:

**Approved General Banner**

* This warning banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this Government system, which includes (1) this computer network, (2) all computers connected to this network, and (3) all devices and storage media attached to this network or to a computer on this network.
* This system is provided for Government-authorized use only.
* Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties.
* Personal use of social media and networking sites on this system is limited as to not interfere with official work duties and is subject to monitoring.
* By using this system, you understand and consent to the following:
  + The Government may monitor, record, and audit your system usage, including usage of personal devices and email systems for official duties or to conduct HHS business. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this system.
  + Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose.

**Size Restricted Banners**

This standard abbreviated warning banner may be used in circumstances where the standard warning banner cannot be implemented, such as when:

* a system has character limitations related to the warning banner display; or
* the standard warning banner is inconsistent with certain directives, policies, regulations, or standards (e.g., requirements governing special-purpose scientific or medical systems or tracking of personal information on publicly accessible websites).

This warning banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this Government system, which includes all devices/storage media attached to this system. This system is provided for Government-authorized use only. Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties. At any time, and for any lawful Government purpose, the government may monitor, record, and audit your system usage and/or intercept, search and seize any communication or data transiting or stored on this system. Therefore, you have no reasonable expectation of privacy. Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose.

## Permitted Actions without Identification and Authentication (i.e., Public Access) (AC-14)

*Identify the permitted user actions that do not require user identification and authentication and provide rationale for permitting such actions.*

*For example: non-authenticated (aka Public) users are permitted anonymous access to the home page of {SYSTEM NAME}, which contains general, non-sensitive information related to XYZ program. Any restricted information that is not intended for the public requires user identification and authentication in accordance with the IA policies set forth earlier in this document. The rationale for allowing this anonymous access is ABC…s*

* Step 1
* Step 2
* Etc.

## Publicly Accessible Content (AC-22)

*Describe the process and/or controls used to control/limit who is authorized to post information to publicly accessible sites/systems; also describe the process for reviewing, approving, and ensuring that no non-public information is posted, and for ensuring that, if discovered, non-public information is promptly removed from public sites/systems.*

* Step 1
* Step 2
* Etc.