ACCESS MANAGEMENT STANDARD – USER ACCOUNT TYPES

The capitalized terms used herein are defined in the Access Management policy.

In accordance with Northern Arizona University's Access Management policy, the Chief Information Officer ("CIO") updates and revises, as necessary and appropriate, a set of Access Standards. These standards establish acceptable practices for the types of accounts defined in this document. The standards apply to all University Community Members and to accounts on all University-owned IT Resources. Contact the CIO or the Identity and Access Management ("IAM") team with any inquiry or feedback regarding these standards.

1. **Individual User Accounts.** Individual user accounts are provisioned to all active University Community Members and are unique per individual. Individual user accounts may serve as domain authentication and can also be referred to as a "Domain" account. Individual user accounts must not be utilized in place of a Service Account or Privileged Access account as defined in this document.
   a. Individual user account holders must not share their authentication credentials. Passwords for Individual user accounts should be unique and in line with the University's Authentication standard.
   b. Student employee access: Student employees should be configured with specific access control rights separate from their individual user account to support separation of employment from other academic responsibilities whenever possible. Separation of access controls may be accomplished with the utilization of persona accounts, access control groups, or role management. This may include, but is not limited to, email account access, University instant messaging services, shared drive access, organizational access, and administrative responsibilities associated with the University.
   c. Account conventions: Individual users are provisioned a unique NAU User ID or NAU UID to work with University resources. To avoid conflicting NAU UIDs, the University provisioning engine generates a combination of the individual's officially recorded initials at date of initial enrollment or employment at the University and may include one or more digits (e.g., xyz123).
      ▪ Username and NAU UID changes: Username changes have strict criteria due to the significant impact on multiple systems across the University. They may require multiple days' worth of accumulated personnel hours to safely update all accounts, databases, and systems appropriately.
      ▪ Criteria for NAU UID change
         ✓ Legal name change - the user must have a legal name change registered with Human Resources or the Office of the Registrar, which must be present in their authoritative PeopleSoft data.
         ✓ Marriage or divorce - NAU UID change requests related to marriage or divorce will not be granted by default. An exception may be requested in the form of a service ticket to the IAM. The user must demonstrate a significant need or justification for the change, which will be evaluated by a Director or CIO on a case-by-case basis.
         ✓ Safety/Stalking - requests related to personal safety or stalking must be confirmed with documentation from University or local police.
         ✓ Gender/Identity change - user must have legal name change registered with the University. Nicknames, aliases, or preferred names are not acceptable for use in creation of a new NAU UID.
         ✓ Vulgar or inappropriate NAU UID - requests that auto-generate NAU UIDs that result in letter or number combinations that are deemed offensive or vulgar, which may include foreign languages, will be evaluated by NAU ITS on a case-by-case basis.
   d. Provisioning and deprovisioning: Individual user accounts will be automatically provisioned and deprovisioned within one of the University's primary directories in line with the individual's current affiliations to the University. Manual provisioning and deprovisioning of user accounts is prohibited unless approved by University Officials.

2. **NAU Guest Accounts.** Guest Accounts are local Windows and Macintosh workstation accounts and are designated for open learning environments.
    a. Account Conventions: Guest Accounts must be named as "NAU Visitor" unless an exception request has been filed with the IAM team. The "NAU Visitor" account will not have any applied password and must not be provided access to other University IT Resources beyond the utilization of public internet access.
    b. Provisioning: Provisioning of NAU Guest Accounts must occur only after an official request has been submitted for review to an appropriate Information Technology Services ("ITS") support team. ITS support teams will review each request to determine appropriateness of the request and, upon approval, will deploy the "NAU Visitor" account policy to the designated machines denoted within the request. All NAU Guest Accounts will be deprovisioned by the date listed in the request and should not be provisioned longer than 10 business days within any consecutive period without an approved exception request on file with the IAM team.
    c. Auditing and Expiration: ITS support teams are responsible for the auditing and expiration of the NAU Guest Accounts that they approved. A yearly audit of all systems configured with NAU Guest Accounts should be performed in a collaborative effort between the ITS support teams and IAM team.

3. **Shared Accounts**: Shared Accounts are shared by one or more users. These accounts are different from user accounts that are associated with a single individual. These accounts should be disabled from workstation or remote login interfaces when possible.
    a. Types of Shared Accounts
        - Lab Accounts: Lab Accounts are Microsoft Active Directory accounts and will be designated for research labs and other environments that have a need for shared login capabilities and forms of persistence, including, but not limited to, storage, software, and configurations. These accounts must be associated with a responsible individual and must not be shared outside of the business unit that requested the account.
            - ✓ Account Conventions: Lab Accounts must be named with a prefix of "L-," followed by the responsible Vice President ("VP") area and descriptor of where and/or what the account is being utilized for, and must not exceed 20 characters in length.
        - Department & Organization Shared Exchange Access Accounts: Department & Organization Shared Exchange Accounts are intended to be used for shared email boxes that may be setup for voicemail access. Account holders must not share the authentication credentials for this account outside of their direct group.
            - ✓ Account Conventions: Department & Organization Shared Exchange Access Accounts must be named with a prefix of "S-," followed by the responsible VP area and descriptor of where and/or for what the account is being utilized, and must not exceed 20 characters in length.
        - Resource Accounts: Resource Accounts are shared accounts designated for physical resources that may have cross department or multi-organization usage.
            - ✓ Account Conventions: Resource Accounts must be named with a prefix of "R-," followed by the responsible VP area, building, and room number of where the account is being utilized, and must not exceed 20 characters in length.
    b. Authentication: Shared Accounts must have a unique password that is no shorter than 12 characters in length. Shared Account passwords should not have a password expiration associated with the account. Passwords must be reset upon the departure of an individual who was granted access to the password or when the password is suspected of being compromised in any fashion.
    c. Provisioning: Provisioning of Shared Accounts must be made via an official request that has been submitted for review to an appropriate ITS support team. ITS support teams must review requests to determine appropriateness of the request and, upon approval, will request the account creation from the team responsible for Microsoft Active Directory account provisioning. Accounts should not be provisioned for longer than one year at a time without an annual review.
    d. Auditing and Expiration: A yearly audit of all shared accounts should be performed in a collaborative effort between the ITS support teams and IAM team.

4. **Device Service Accounts**: Device Service Accounts are Microsoft Active Directory ("AD") accounts, are designated for devices such as Internet of Things and printer devices that will need access to domain resources, and not associated with a particular individual.
    a. Account Conventions: Device Service Accounts must be prefixed with "D-," followed by the descriptor of what the device is and where it will be primarily located, and must not exceed 20 characters in length. Passwords for these accounts must be no shorter than 12 characters in length.

b. Provisioning: Provisioning of Device Service Accounts must have an official request that has been submitted for review to an appropriate ITS support team. ITS support teams must review requests to determine appropriateness of the request and, upon approval, will request the account creation from the team responsible for Microsoft AD account provisioning.

c. Auditing and Expiration: A yearly audit of all Device Service Accounts should be performed in a collaborative effort between the ITS support teams and IAM team.

5. **Service Accounts for Server Operating Systems:** Service Accounts are domain accounts designated to monitor, administrate, maintain, or test applications within a controlled environment. Service Accounts must not be shared outside of the business unit that requested the account. Service Accounts must be associated with a responsible individual or group. These accounts should be disabled from workstation or remote login interfaces when possible.

   a. Types of Service Accounts
      - Service Account: Service Accounts are user accounts created explicitly to administer services running on Windows Server operating systems. These accounts determine the ability to access local and network resources.
        - ✓ Account Conventions: Service Accounts will be prefixed with “Srv-” and must not exceed 20 characters in length. Service Accounts will have a unique password that is no shorter than 127 characters in length, unless unsupported by the server; in that case, the maximum supported character length for a password will be applied. Passwords will not have an explicit expiration but should be changed upon the departure of any personnel who was granted access to the password or when the password is suspected of being compromised in any fashion.
      - Group Managed Service Accounts (“GMSAs”): GMSAs provide a higher security option than Service Accounts for non-interactive applications, services, processes, and tasks that run automatically but need security credentials on Windows systems.
        - ✓ Account Conventions: GMSAs will be prefixed with “GMSA-,” the name of the application, and the application component with which it is intended to be used. These accounts are not intended for human interaction and will not have an authentication method that individuals can interact with.
      - Service Testing Accounts: Service Testing Accounts are designated for temporary access to services to accommodate testing of services outside of the utilization of an Individual User Account. Service Testing Accounts will be associated with a specific individual and must be expired within 30 days from date of creation.
        - ✓ Account Conventions: Service Testing Accounts must be prefixed with “SrvTest-,” followed by the name of the service that is being tested, and must not exceed 20 characters in length. Service Testing Accounts must have a unique password that is no shorter than 127 characters in length, unless unsupported by the server; in that case, the maximum supported character length for a password will be applied.
      - Application Service Accounts: Application Service Accounts are designated for the operation of applications separate from the operational maintenance of the server operating system.
        - ✓ Account Conventions
          (a) Microsoft: Microsoft Application Service Accounts must be prefixed with “SrvApp-,” followed by the application and role that for which the Service Account is being utilized, and must not exceed 20 characters in length. Microsoft Application Service Accounts must have a unique password that is no shorter than 127 characters in length, unless unsupported by the server; in that case, the maximum supported character length for a password will be applied.
          (b) LDAP: LDAP Service Accounts or Application DNs must be named in a unique fashion that is relevant to the application and role that the service account is being utilized for. Application DNs must have a unique password that is no shorter than 16 characters in length.

   b. Provisioning: Provisioning of Service Accounts must be performed by an approved provisioning process under the guidance of IAM. The creation of Service Accounts outside of approved mechanisms and methods is expressly prohibited.

   c. Auditing and Expiration
      - Annual auditing: All Service Accounts must be audited on an annual basis to evaluate the continued need and operational efficiency of the account.

        - Employee Separation: Accounts that have an associated password must change the password upon the separation of any personnel that were previously granted access to the password whether, in clear text or stored with in a password management system.

6. **Persona Accounts**: Persona Accounts are additional accounts intended to be utilized by personnel that require separation of access or administrative abilities on multiple systems.
    a. Account Conventions: Persona Accounts must be named with the individuals NAU UID followed by a predefined suffix on record with IAM.
        - Persona Accounts should be authenticated with a form of multifactor authentication when available.
        - Password must be greater than 12-characters in length. Passwords for Persona Accounts must be unique from non-privileged accounts and not re-used.
        - Persona Accounts should not be used to browse the internet, access email, open attachments, or perform other day-to-day common user activities.
        - Persona Account credentials must never be shared.
        - Authentication methods in which Persona Account information is passed un-encrypted in “plain-text,” such as telnet or ftp, are not permitted.

    b. Provisioning: Provisioning of Persona Accounts must be performed by an approved provisioning process under the guidance of IAM and must have an approved request on record prior to the creation of the account. The creation of Persona Accounts outside of approved mechanisms and methods is expressly prohibited.

    c. Auditing and Expiration: All persona Accounts must be audited on an annual basis to determine the continued need for separate or elevated privileges. Persona Accounts will be expired upon the conclusion of an individual’s employment or upon change of job duties that no longer require separate or elevated privileges.

7. **Local System Accounts**: Local System Accounts are accounts that are not associated with any of the University’s domains and only have access to the local system on which they reside.
    a. Account Conventions
        - Workstations
            - ✓ Windows
                (a) Administrator Account: The Windows operating systems default administrator account must be disabled. A secondary local user administrator account must be created and named as 1899. This account must have its password changed on a weekly basis to a randomized password no shorter than 12 characters in length. The password for this account will be stored as part of the machine object in Microsoft AD as a secured attribute value.

                (b) User Accounts: The utilization of local user accounts is prohibited without an approved exception request on file with the IAM team.
            - ✓ Macintosh (Mac)
                (a) ITS Administrator Account: Macs should have an administrator account named Administrator. This account should have its password changed on a weekly basis to a randomized password no shorter than 12 characters in length. The password for this account will be stored as part of the machine object in Microsoft AD as a secured attribute value.

                (b) User Accounts: Macs should not have local user accounts without an approved exception request on file with the IAM team.
        - Servers
            - ✓ Windows Server
                (a) Administrator Account: The Windows server operating systems default administrator account must be renamed from any standard account name including, “Admin”, “Administrator”, and “Root”. This account must have its password changed on a weekly basis to a randomized password no shorter than 16 characters in length. The password for this account will be stored as part of the machine object in Microsoft AD as an encrypted attribute value.

                (b) User Accounts: The utilization of local user accounts is prohibited without an approved exception request on file with the IAM team.
            - ✓ Linux and Unix Servers
                (a) Root: Root user accounts should not have the ability to SSH into the system. Root user accounts must have a password no shorter than 16 characters in length. Passwords will not have an explicit expiration but should be changed upon the departure of any personnel that

was granted access to the password or when the password is suspected of being compromised in any fashion.

(b) User Accounts: User accounts should not be configured with administrative abilities and must utilize “sudo” to elevate system level access. User accounts must have a password that is no shorter than 12 characters in length. Passwords will not have an explicit expiration but should be changed upon the departure of any personnel that was granted access to the password or when the password is suspected of being compromised in any fashion.

- Applications and Hardware Appliances
  - ✓ Hardware Appliances: Hardware appliances should have a password that is at least 16 characters in length, unless otherwise unsupported on the appliance itself. Passwords are not required to expire or change upon the departure of personnel but must be updated if found as part of a compromise. User account passwords must be changed from the default user account password that the device is shipped with.
  - ✓ Vendor Applications: Vendor application accounts that are not federated to one of the University’s authentication systems should be associated to a member of the University by the use of at least one of the following attributes in descending order of precedence: (1) NAUEDURegID; (2) NAU User ID; or (3) NAU Email Address. These accounts must not reutilize the password associated with the users NAU User ID.

b. Provisioning: Provisioning and creation of accounts must be performed by an IAM approved provisioning process.

c. Auditing and Expiration: A yearly audit of all accounts should be performed in a collaborative effort between the ITS support teams and IAM.

8. **Expiration and Auditing of Exceptions Requests:** An annual audit of exceptions will be conducted to validate that the continued need and validation of business justification against the University’s current security practices. ITS support teams will be responsible for the periodic auditing of all NAU Guest Accounts to validate that deprovisioning has occurred in accordance with the provisioning best practices stated in Section 2 of this standard.