N-04: Active Directory Accounts

POLICY: See HHSA-N-04 Active Directory Accounts – Management & Use, at www.cosdcompliance.org.

DEFINITIONS: See HHSA Policy N-13 Security Definitions.

PROCEDURES:

1. County Computer Account Responsibilities
    a. Users are responsible for taking reasonable care to protect their Active Directory (AD) Account and associated credentials, including not sharing credentials or permitting others to use their account. Users are responsible for all activity performed on their assigned AD account.
        i. If a user suspects their AD account has been compromised, they must immediately change their password (if able) and notify their supervisor and the IT Service Desk.
    b. Accounts that remain inactive beyond established County thresholds may be automatically disabled and require reactivation through approved access management process.
    c. Prior to accessing County information systems and data, users are responsible for completing required privacy and security awareness training and complying with applicable County and HHSA policies and procedures.
2. County Positions Covered by Auto-Provisioning
    a. For County positions maintained in PeopleSoft, AD account status and default access are managed through the auto-provisioning process. Positions covered by auto-provisioning included:
        i. Standard County employees
        ii. Unclassified executives
        iii. Management fellow
        iv. Student workers (High School, Undergraduate, Graduate/Tech)
        v. Temporary employees (e.g. certified temp, retired rehire, temp expert professional)
    b. Account Creation (Auto-Provisioning)
        i. For new hires or rehires, AD accounts are automatically created based on the effective hire date entered in PeopleSoft and include:
            1. A unique AD/windows username
            2. Office365 account and access (e.g., Outlook, OneDrive, SharePoint, Teams)
            3. Remote Access/Akamai EAA
            4. Required County security controls (e.g., password expiration, lockout thresholds)
            5. Default access associated with the department is based on the applicable

Auto-Provisioning Default Group List. Refer to ServiceNow Knowledge KB0014070, *Auto-Provisioning Default Group List*, for additional details regarding default access assignments.

ii. Departments are responsible for submitting access requests to grant, modify, or remove non-default access based on assigned job duties. Access should be limited to the minimum access necessary to perform assigned job functions.

c. Training Requirement
   i. Employees must complete privacy and security awareness training within 30 days of initial AD login and annually thereafter.

d. Leave of Absence:
   i. When an employee begins an approved leave, the AD account is automatically blocked based on the PeopleSoft effective leave date.
   ii. Microsoft 365 services are not separately disabled when the AD account is blocked. However, the user cannot authenticate, and access to connected services is unavailable until the account is re-enabled.

e. Return of Absence:
   i. Upon return, the AD account is automatically re-enabled based on the PeopleSoft effective return date.

f. Transfers within HHSA
   i. When a county employee transfers to another HHSA program or unit, auto-provisioning updates the AD account based on the effective date in PeopleSoft. The following actions occur:
      1. Default access for the previous Department is automatically removed.
      2. Default access for the new Department is automatically applied.
      3. The employee's OneDrive remains associated with the employee and will follow the employee when transferring within HHSA.
      4. The employee's former Department is responsible for submitting timely requests to remove or modify any non-default or elevated access (e.g., third-party application roles, SharePoint/Teams access, MS licenses such as Power BI or Visio).
   ii. Departments must coordinate to ensure prior non-default or elevated access is appropriately removed and that County-assigned resources are appropriately transferred or removed.

g. Transfers Out of HHSA:
   i. When an employee transfers to another County Group, default access associated with the employee's HHSA organizational assignment is automatically removed through the auto-provisioning process.

ii. The HHSA OneDrive will remain under HHSA ownership and will not transfer with the employee. The employee will be assigned a new OneDrive by the receiving County Group. If access to or a copy of the HHSA OneDrive content is needed, contact Agency DHRO for assistance.

iii. The employee's former HHSA Department remains responsible for submitting timely requests to remove any non-default or elevated access and that County-assigned resources are appropriately transferred or removed.

h. Separation or Termination:

i. When employment ends, the AD account is automatically deleted based on the separation date in PeopleSoft. Associated OneDrive content is archived for 60 days and then permanently deleted. If access to an Archive drive is needed, refer to Department DHRO.

ii. Departments are responsible for reviewing and removing any non-default, elevated, or third-party application access that is not automatically managed through the AD account lifecycle process, including applications that do not integrate with County Single Sign-On (SSO).

3. Non-County Positions Not Covered by Auto-Provisioning

a. Non-County positions not included in PeopleSoft do not undergo auto-provisioning and require full manual management. These include:

i. Contingent Workers (e.g., external agency temp staff, contract workers, independent consultants)

ii. Volunteers

iii. Vendor Personnel

iv. Non-County hired student interns

b. Eligibility and Agreement Requirements

i. An active contract, agreement, MOA/MOU, or other formal arrangement must be in effect before an AD account be created for HHSA Non-County staff.

ii. Non-County AD accounts must be assigned an expiration date not to exceed 12 months or the contract/agreement end date, whichever is sooner. The County sponsor must recertify the account before extending access.

c. Manual Account Management

i. The County sponsor is responsible for submitting access requests in a timely manner to:

1. Create the AD account
2. Modify access
3. Terminate access
4. Recertify or extend the account before expiration

ii. The sponsor must ensure the level of access remains appropriate and minimum necessary to perform assigned job functions.

d. Remote Access Requirements
   i. Non-County staff requesting remote access must follow the County's Third-Party Access Request (TPAR) process or other approved access management process to identify and approve the minimum access necessary to perform assigned job functions prior to remote access being granted.
   ii. Approved remote access may require County-issued equipment, membership in designated remote access groups, or other County-approved security controls.
   iii. Personal devices may not be used unless explicitly approved under County remote access standards.

4. Notice on Computer Account Use Monitoring and Enforcement
   a. Users have no expectation of privacy when using County systems, networks, or devices. Any data or information created, accessed, received, stored, deleted, or sent via County's information systems must not be considered private or confidential as the County reserves the right to monitor, access, retrieve, restore, delete, or disclose any data or activity at any time.
   b. Violations or suspected violations of this procedure may be referred to management for review and appropriate follow-up, which may include referral to Agency Human Resources and/or legal review.
5. Additional Guidance
   a. Users should also reference County of San Diego Administrative Manual Item 0400-03, Computer Accounts – Management and Use, for additional requirements related to County computer accounts.

QUESTIONS/INFORMATION: Please contact HHSA Business Assurance and Compliance (BAC) by email at Compliance.HHSA@SDCounty.ca.gov or by phone (619) 237-8571.