COUNTY OF SAN DIEGO
Health and Human Services Agency

LIVE WELL SAN DIEGO

# N - 03: Passwords Management & Use

**POLICY:** See HHSA-N-03 Passwords, at www.cosdcompliance.org.

**DEFINITIONS**: See HHSA Policy N-13 Security Definitions.

**PROCEDURES:**

1. General Requirements
    a. Each user must have a unique County user ID and password.
    b. Users are responsible for all activities under their assigned account.
    c. Passwords must:
        i. Meet County complexity standards.
        ii. Be memorable without needing to be written down.
        iii. Be different from those used for personal accounts (e.g. banking, Gmail).
        iv. Use different passwords for multiple systems (do not reuse the same password across systems).
2. Prohibited Practices
    a. Users shall not:
        i. Share their passwords with anyone under any circumstances.
        ii. Use another person's ID/password (including those transferring out, on vacation, extended leave, or no longer employed).

            ***NOTE:*** Contact the Department DHRO for assistance if access to the owner's emails or files needs to be retrieved after the employee has left. Note, business justification will be required.

        iii. Allow browsers or applications to save, remember, or automatically fill in your County passwords. *You must manually enter each time to keep your account secure.*
3. Password Complexity
    a. Password length must conform with the County standard found in CAO Administrative Policy 0400-04.
    b. Cannot contain the user's account name, full name, or other personally identifiable information.
        i. For telephones and smartphones, passcodes/PINS must not include easily guessed numbers (e.g., the device's phone number or 1234).
    c. Must include at least one character from the following four groups:
        i. Uppercase letters (A-Z).
        ii. Lowercase letters (a-z).

iii. Numbers (0-9).

iv. Special characters (e.g., ! @ $ % ^ & *).

d. A passphrase may be used instead of a traditional password, provided it meets County complexity requirements. Passphrases should be long (e.g., fifteen (15) or more characters), memorable, and composed of multiple unrelated words or a phrase that is not easily guessed.

4. Password Maintenance

a. Passwords must be changed immediately after the first issuance.

b. Passwords must be updated periodically per the County Information Security Plan (ISP).

c. A password must not be reused.

d. Users must change their password and report unusual activity if they suspect compromise.

i. On your keyboard, press CTRL + ALT + DEL simultaneously, then select “Change Password”.

e. After multiple failed login attempts, accounts will be locked automatically. The account owner is to contact the appropriate system administrator to unlock or request a password reset.

5. Password Resets

**a. County Employees**

i. Are responsible for resetting their own network passwords.

ii. Password resets and MFA unblocking must be requested directly through the ServiceNow Help Desk.

iii. This includes requests following account lockouts.

**b. Password Reset Authorizers (PRA)**

i. PRAs must be current County employees and approved by their Department Manager or Supervisor before being designated in ServiceNow.

a. If a user is no longer fulfilling the PRA role, a ServiceNow ticket must be submitted to remove them from the PRA List.

ii. PRAs are designated to support Windows network accounts (passwords) for non-County users only, and may support only the Department, Division, or Low Org(s) to which they are assigned.

iii. The user’s identity must be verified each time before a password reset or unblock request is processed.

iv. Capabilities

a. May request password resets on behalf of non-County users.

b. May request MFA unblocking of non-County user accounts blocked due to a lack of or unregistered MFA device.

v. Limitations

a. Cannot request password resets for County employees. Employees must contact the ServiceNow Help Desk.

b. Cannot request unblocking of County employee MFA devices. Employees must contact the ServiceNow Help Desk.

c. **Non-County Users not in PeopleSoft (e.g., Contingent Workers, Vendors)**
   i. Must contact their designated County sponsor to request a password reset.
   ii. The County sponsor verifies the individual's identity and then requests a password reset through the appropriate Password Reset Authorizer or system administrator.

6. Mobile Devices
   a. Devices (e.g., smartphones, tablets) accessing County data must be enrolled in County Mobile Devices Management (MDM).
   b. Biometric authentication (e.g., fingerprint, face ID) may be used, but a compliant password must also be set.
7. Third-Party Systems
   a. This policy applies to County-managed accounts and systems.
   b. Staff who use third-party or vendor-managed systems not managed via single-sign on (SSO) (e.g., state, federal, or external partner applications) for County business are expected to:
      i. Follow the password reset protocols established by the system owner or vendor.
         a. At minimum, any third-party solutions used for County business must allow passwords for applications and service accounts to be changed on a regular basis (at least annually), including all default administrator passwords. If the vendor requires passwords to be changed more often, staff must follow those requirements.
      ii. Apply the same best practices described in Sections 1-4 (General Requirements, Prohibited Practices, Password Complexity, and Password Maintenance) to the extent possible including:
         a. Creating strong, complex passwords.
         b. Protecting passwords from disclosure or reuse.
         c. Regularly updating passwords and monitoring for unusual activity.
8. Violations
   a. Suspected or confirmed violations of this procedure involving County-managed accounts or systems may result in disciplinary action, including referral to Agency Human Resources for further investigation and appropriate personnel action.
   b. Misuse of third-party or vendor-managed systems while conducting County business may also be subject to review, investigation, and reporting to the appropriate County management, vendor, or governing body.

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