

**CDPH-ISO/DHCS-ISO**  
**Account & Password Policy**

**IV.C.12. Username/Password Based Authentication**

When usernames and passwords are going to be used as the method for system authentication the following for each must be met:

- Username requirements:
  - Usernames are unique and are traceable to an individual worker.
  - Usernames are NOT to be shared and never hard-coded into system logic.
  
- Password requirements:
  - Are not to be shared.
  - Must be 8 characters or more in length.
  - Must NOT be a word found in the dictionary, regardless of language.
  - Passwords must be encrypted using irreversible industry-accepted strong encryption.
  - Must be changed at least every 60 days.
  - Must NOT be the same as any of the previous 10 passwords.
  - Must be changed immediately if revealed or compromised.
  - Must be composed of characters from at least three of the following four groups from the standard keyboard:
    - Upper case letters (A-Z);
    - Lower case letters (a-z);
    - Arabic numerals (0 through 9); and
    - Non-alphanumeric characters (punctuation symbols).
  - Accounts must be locked after 3 failed logon attempts.
  - Account lock-out reset timers must be set for a minimum of 15 minutes.

**IV.C.13. Privileged Accounts Management**

- Privileged Account Authorization  
A privileged account is an account that allows an individual to perform maintenance on an operating system or application (e.g. create/remove users, install applications, create/modify databases). Privileged accounts require the approval of the individual's manager, the ISO, and must include a business justification stating why privileged access is required and what it will be used for. Individuals granted privileged accounts must have already signed the Security and Confidentiality Acknowledgement Statement. Privileged accounts must be unique and associated with the individual for whom the account is authorized. The use of shared privileged accounts (e.g. Administrator) is strictly prohibited.
  
- Username requirements
  - Must be unique and are traceable to an individual person.
  - Must NOT be shared.
  - Must never be hard-coded into system logic.
  - Must NOT be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
  - The default built-in Administrator account must be renamed and disabled.

- The naming convention for privileged accounts must not make it obvious that usernames belong to privileged accounts.
- If a generic privileged account is created:
  - It must only be used in an Emergency.
  - It is NOT to be used for routine maintenance.
  - The password storage and management process for generic privileged accounts must be approved by the Department ISO.
- Password requirements
  - Must not be the same as any of the previous 10 passwords.
  - Must not to be shared.
  - Must NOT be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
  - Must be 12 characters or more in length.
  - Must NOT be a word found in the dictionary, regardless of language.
  - Password must NOT be stored in clear text.
  - Must be changed at least every 60 days.
  - Must be changed immediately if revealed, or compromised.
  - Must be changed immediately upon the termination or transfer of an employee with knowledge of the password.
  - Passwords must be encrypted using industry accepted, irreversible strong encryption.
  - Accounts must be locked after 3 failed logon attempts.
  - Account lock-out timers must be set for at least 60 minutes.
  - Must be comprised of characters from at least three of the following four groups from the standard keyboard:
    - Upper case letters (A-Z);
    - Lower case letters (a-z);
    - Arabic numerals (0 through 9);
    - Non-alphanumeric characters (punctuation symbols).
- Restrictions for Privileged Accounts
  - Holders of privileged accounts must restrict the use of their account privileges to activities that are part of their job and that require privileged access.
  - Holders of privileged accounts must never share their access and password with other individuals.

#### **IV.C.14. Service Accounts Management**

- Service Account Authorization
 

In situations where it is necessary to use a service account, which is an account used to run a service and whose password is known by multiple individuals, the account request will be approved by the manager of the Project/Program requesting the account and by the ISO. Requirements, stating the need for a service account, will be documented in the request. A service account password is shared among the individuals authorized to access the account, and is subject to controls as stated in the password requirements in this document.
- Restrictions for Service Accounts

- Sharing passwords via email is prohibited, unless the body of the email itself is encrypted using strong encryption.
- When users are no longer authorized to access an existing service account, the service account password must be changed.