COUNTY OF IMPERIAL
DEPARTMENT OF BEHAVIORAL HEALTH SERVICES

POLICY AND PROCEDURE MANUAL

SUBJECT: HIPAA - Password and User Identification (ID) Controls	**POLICY:** 01-100
SECTION: Administration	**EFFECTIVE DATE:** 10-14-15
REFERENCE: 45 C.F.R. Section 164.308(a)(5)(ii)(D); 45 C.F.R. Section 164 308 (a)(5)(ii)(D), DHCS Contract	**PAGE:** 1 of 4 **SUPERSEDES:** 8-29-12
AUTHORITY: Behavioral Health Director as the Local Mental Health Director and Alcohol and Drug Administrator	**APPROVED BY:** Andrea Kuhlen

PURPOSE: To establish a standard for creating and protecting strong unique user IDs and passwords and the frequency of change.

NOTES: Passwords are an important aspect of computer security. Used in combination with unique users identifications, passwords are the front line of protection for the ICBHS informations system. A poorly chosen password may result in the compromise of sensitive or confidential information.

SCOPE: All ICBHS users, including contractors and vendors with access to ICBHS systems, are responsible for taking appropriate steps, as outlined below, to select and secure their passwords.

DEFINITIONS: Password: means confidential authentication information composed of a string of characters

User: means a person or entity with authorized access.

User ID: The user name or username by which a person is identified to a computer system or network. A user commonly must enter bother a user ID and a password as an authentication mechanism during the logon process.

Policy Owner: Security Officer

POLICY: User IDs and passwords are required in order to gain access to ICBHS systems, networks, and data. Users are required to select a password to obtain access to any electronic information both at the server and workstation level. Users are responsible for the security of their passwords.

1. <u>Unique User Identification</u>

   All new users must attend an Avatar orientation training prior to being assigned a unique user name and password.

   The user name must be used only by the assigned user and is not to be shared. Authorized users are responsible for activities taken using their assigned user identification and password.

2. <u>Password Criteria</u>

   Passwords must meet all the following criteria.

   a. <u>Length.</u> All passwords must be eight characters in length.

   b. <u>Complexity Requirement</u>
   Passwords shall be composed of characters from all of the following three groups.

      1) Upper case letters (A-Z)

      2) Lower case (a-z)

      3) Arabic numerals (0-9).

   c. <u>Passwords</u>
   Passwords shall not be constructed by using personal information or dictionary words. Examples of personal information include a spouse's name, children's names, automobile license number, social security number, or birthday, etc.

   d. <u>Password History</u>
   Passwords used in the past cannot be reused.

3. <u>Password Disclosure</u>

   a. <u>Recording Passwords.</u> Passwords must not be written or otherwise recorded in a readable format where they are accessible or recognizable by anyone else, such as taped to computer screens, stored under keyboards, or otherwise visible in a work area.

b. Sharing Passwords. Passwords shall not be shared or used by others. This includes co-workers, manager, supervisor, friend, vendors, county information systems staff. On rare occasions, passwords may need to be shared with the IT staff during a troubleshooting process. Once the troubleshooting process is complete, users must change their passwords to that it is only know to them.

c. "Remembering Password" features. Features that allow applications or systems to "remember" passwords shall not be used.

d. Revealed or Compromised Passwords. A password shall be changed immediately when it has been revealed or compromised, or when there is suspicion that it has been revealed or compromised.

4. Password Control

a. Initial Passwords. Initial passwords issued by the systems administrator shall be valid only for the first log-on. Users will be prompted to create unique passwords at the first log-on.

b. Invalid Password Attempts Workstations, servers, and network devices are configured to lock out a user account after three invalid password attempts.

c. Password Changes. Passwords shall be changed every ninety (90) days.

d. Password Termination. Upon notification of an employee's termination, transfer, or resignation from the ICBHS Human Resource Unit, the Behavioral Health Manager for Information Systems or designee shall promptly inactivate the employee's password.

e. Default Passwords. Default passwords must be changed before any devices or software in placed in service.

5. Compliance

Failure to comply with this policy and associated procedure(s) may result in disciplinary action up to and including termination.

Related Policies and Regulations

Policies:

1. Security Management Policy
01-231 Access Control Policy

Regulations:

1. 45 C.F.R. Section 164.308 (a)(5)(i): Standard: Security Awareness and Training. Implement a security awareness and training program for all members of its workforce (including management).

2. 45 C.F.R. Section 164.308 (a)(5)(ii)(D): Password Management (Adressable). Procedures for creating, changing, and safeguardinig passwords.