County of San Bernardino
Department of Behavioral Health

User- I.D. and Password Policy

Effective Date 1/29/07
Approval Date 1/29/07

Allan Rawland, Director

Policy

The Department of Behavioral Health (DBH) will use standardized User-I.D.'s and passwords to protect its systems and data from unauthorized access in accordance with Departmental, County, State, and Federal requirements to preserve the confidentiality of client related electronic data.

Purpose

To establish staff responsibilities and a method for tracking data access by the issuance of User-I.D.'s and passwords, which will protect the integrity, vulnerability, and unauthorized access of DBH data.

General Information

Staff requiring access to DBH systems will be assigned one or more unique User-I.D.'s based on daily job duties. Each User-I.D. will have a unique password that must not be shared between staff.

Staff Responsibilities

The following are the responsibilities of the staff:

Staff	Responsibilities
Manager/Supervisor	• Request staff authorizations in writing to Information Services (IT) and provide: ○ Employee name ○ Employee county identification number ○ Unit or clinic to which employee is assigned ○ Application(s) to which access is required ○ Level of responsibility and need to know confidential client information • Notify IT if there is a change to an employee's level of responsibility.

Staff	Responsibilities
Information Services	• Establish a User-I.D. and first-time temporary password for network access for new staff members only. • Establish a User-I.D. and first time temporary password for each requested application based upon level of responsibility. • Notify staff member of assigned User-I.D. and temporary password. • Reset staff passwords if they have been compromised or forgotten • Disable, reestablish, or terminate a staff member's access based upon a written and/or oral request from management. • Notify the department's Privacy Officer of each access granted and removed

Staff	• Select a new password when prompted upon initial sign-on to the network and/or application.
	• Passwords must have a minimum length of seven characters and contain two of the three following characteristics:
	  ○ One upper and lower case alphabetic character
	  ○ One numeric character
	  ○ One special character such as; $, #, @
	• Keep all passwords secure.
	• Change passwords every ninety (90) days or when prompted by the system.
	• Notify IT if locked out of the system and require a password reset.

Management/Human Resources	• Notify IT in writing if a staff's access should be terminated, disabled, or reinstated. ○ Oral notification is acceptable if action is to be taken immediately.

Consequences of Violations

Staff who violates the use of DBH systems as described above or in other County policies will be subject to disciplinary action that can include termination of employment.