SAN BERNARDINO COUNTY
Behavioral Health
303 E. Vanderbilt Way San Bernardino | (909) 388-0900
***www.SBCounty.gov***

# Information Technology Account Management Policy

| | | |
|---|---|---|
| **Approval Date** | 01/23/2025 | DocuSigned by: Dr. Georgina Yoshioka 7DF8077EFA674B2... |
| **Effective Date** | 01/23/2025 | Georgina Yoshioka, DSW, MBA, LCSW, Director |

**Policy**

It is the policy of the Department of Behavioral Health (DBH) to provide effective management of DBH Information Technology (DBH-IT) Accounts. This policy applies to employees, contractors, temporary and other workforce members at DBH offices who require authorized access to internal network information and software applications and the management of those accounts.

**Purpose**

The purpose of this policy is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at DBH.

**Definition(s)**

**Account**: Any combination of a User ID (sometimes referred to as a username) and a password that grants an individual user access to a computer, an application, the network, or any other information or technology resource.

**Account Issuance, Monitoring, Disabling and Removal**

**Issuing Accounts**

- DBH-IT shall make decisions regarding access to data. Account setup and modification require the approval of the requestor's supervisor;
- Access to ePHI shall not be granted to any person prior to reading and signing an Oath of Confidentiality;
- The activation of accounts as well as the application of appropriate security classes will follow the principle of “least required access” to perform their business function;
- The account managers (server support organization) responsible for an information or technology resource is also responsible for the prompt deactivation of accounts when necessary. For Example, accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment in accordance with the **Employee Separation Procedure** (HR4006) or when continued access is no longer required. The accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location;

*Continued on next page*

| | |
|---|---|
| **Account Issuance, Monitoring, Disabling and Removal** (Continued) | • The identity of users must be authenticated before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that, in totality, could only be known by the account holder. In addition, it is highly recommended stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access;<br>• Temporary passwords for new accounts should only be emailed to remote users through an encrypted and secure channel, and<br>• The date when the account was issued will be recorded in an audit log.<br><br>**Managing Accounts**<br>• All accounts shall be reviewed at least annually by DBH-IT. DBH-IT may also conduct periodic reviews for any system connected to the DBH network, and<br>• All guest accounts (for those who are not members of DBH or contract providers) with access to DBH computing resources shall expire one year or the work completion date, whichever occurs first.<br><br>**Disabling/Revoking/Deleting Accounts**<br>• Accounts may be disabled, revoked or deleted if account privileges are no longer commensurate with an individual's function at the facility or their need-to-know due to changes in their status;<br>• Accounts may be disabled, revoked, or deleted if it is determined the account has been compromised or misused and may only be reinstated at the direction of the DBH Deputy Director over Information Technology;<br>• Under normal circumstances, accounts will deactivate under the following schedule:<br>  ○ Employee (Facility/Staff) Accounts - point of termination;<br>  ○ Consultants and other outside individuals - Until the accounts are no longer needed, and<br>  ○ All Other Accounts - Until the account is no longer needed. |

*Continued on next page*

**Application Security Precautions**

Application developed at DBH or purchased from a vendor should contain the following security precautions:

- Comply with DBH-IT User I.D and Password Policy (IT5009), Data Integrity Policy (COM0925) and Workstation and System Security Policy (COM0924);
- Where technically or administratively feasible, shared ID authentication should not be permitted;
- Authentication should occur external to an application (i.e., applications should NOT implement their own authentication mechanism). External authentication services should be relied upon and provided by the host operating system, the webserver, or the servlet container.
- Passwords must not be stored in clear text or any easily reversible form, and
- Role-based access controls should be used to support changes in staff or assigned duties.

***Note:*** Systems should allow for lockouts after a set number of failed login attempts. Access should then be locked for a minimum of fifteen minutes, unless a local system administrator intercedes. Lock-outs should be logged.

**Compliance**

All users of DBH Information Technology Accounts are required to comply with this policy. DBH-IT reserves the right to deny, to limit, to restrict or extend privileges and access to its Information Technology Accounts.

**Related Policies and Procedures**

DBH Standard Practice Manual and Departmental Forms:

- Workstation and System Security Policy (COM0924)
- Data Integrity Policy (COM0925)
- User I.D and Password Policy (IT5009)

**References**

- Health Insurance Portability and Accountability Act (HIPAA) of 1996 Part 160 and 164
- NIST Digital Identity Guidelines, Special Publication 800-63 (A-B).