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

System Administrator Account Policy

Approval Date	09/08/2025	DocuSigned by: Dr. Georgina Yoshioka 7DF8077EFA674B2...
Effective Date	09/08/2025	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) System Administration accounts of all DBH employees, contractors, consultants, and other workforce members, including all personnel affiliated with a third party to access DBH systems.

Purpose

The purpose of this policy is to provide instruction for Systems Administration accounts to describe associated responsibilities and acceptable use for the various databases, applications, networks, and systems supported within DBH. This pertains to unique and generic system administrator accounts that are built into DBH IT systems.

Definition(s)

IT Systems: A collection of hardware, software, and networks used to collect, process, store, and distribute information to support business operations and decision making.

System Administrator Account: A user account that allows System Administrators to make changes that can affect other users. Administrators can change security settings, install software, add hardware, and access all files on the computer.

Responsibility of System Administrators

Service account and system administrator account access activation shall be approved by DBH-IT Security and enabled by the Server Team. System administrators configure, manage, administer, and monitor DBH computers and other electronic communications hardware and software. They are responsible for:

a. Setting up and documenting service account activations for individuals to access information and services;
b. Helping to resolve problems with usernames and passwords;
c. Researching and resolving problems;
d. Configuring systems and services to the needs of DBH;
e. Monitoring the performance of systems and services;
f. Taking corrective action to improve performance;
g. Implementing corrections and upgrades to provide new features and enhancements;
h. Maintaining system integrity, including but not limited to, tracking malware, investigating security incidents, and performing ordinary system repair, maintenance, and enhancements;

Continued on next page

Responsibility of System Administrators, continued

i. Identifying internal and external risks to the security, confidentiality, integrity, and availability of information in accordance with 45 CFR 164.308(a)(1)(ii)(A);
j. Evaluating the effectiveness of current safeguards for controlling security risks and designing and implementing safeguard programs;
k. Regularly monitoring and testing the safeguard programs (45 CFR 164.308(a)(8)), and
l. Participating in IT systems contingency planning (45 CFR 164.308(a)(7)(i)).

Consequences of Violations

System Administrators who improperly read, disseminate, or otherwise compromise the confidentiality of the electronic system or other data, files, or records will be subject to disciplinary action.

Suspected violations of this policy should be reported to the Office of Compliance and the DBH-IT Management team.

Related Policy or Procedure

San Bernardino County Policy Manual:

- Protection of Individually Identifiable Health Information (16-02)
- Protections of Individually Identifiable Health Information (16-02SP1)

DBH Standard Practice Manual and Departmental Forms:

- Data Integrity Policy (COM0925)
- Privacy and Security Incident Policy (COM0944)
- Electronic Email Policy (IT5005)
- Remote Access Policy (IT5006)
- Device and Media Controls Policy (IT5008)
- User I.D. and Password Policy (IT5009)

References

Health Insurance Portability and Accountability Act, Privacy Rule
NIST Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication 800-53 Revision 4.