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

Internet Account Policy

Effective Date	09/18/2006	DocuSigned by: Dr. Georgina Yoshioka 7DF8077EFA674B2...
Revised Date	04/08/2025	Georgina Yoshioka, DSW, MBA, LCSW, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to provide standardized Internet Access accounts for the DBH workforce in accordance with their assigned roles within DBH.

Purpose

To provide an effective solution for granting appropriate Internet authorizations to allow employees requiring access to the internet via the World Wide Web (WWW) to complete assigned responsibilities.

Definitions

Firewall: A network security device designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules.

Internet: A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Modem: A combined device for modulation and demodulation, for example, between the digital data of a computer and the analogue signal of a phone line.

Authorized Use

Examples of appropriate DBH business use of the Internet include:

- Performing essential job functions;
- Participating in job-related conferences and discussions or collaborating via resources such as websites, newsgroups, chats, and bulletin boards;
- Performing research, obtaining information or support, or pursuing approved job-related education, and
- Promoting and communicating County, DBH, and other business or related information.

Continued on next page

Internet Use

Unrestricted use of the Internet for non-DBH business purposes is prohibited, occasional personal use of the Internet is allowed when such use:

- Is not on DBH work time;
- Does not violate any prohibited activities contained in the DBH Standard Practice Manual or Code of Conduct, and
- Does not interfere with DBH resources or conducting DBH business.

Prohibited Activities

Inappropriate use of the Internet through the County system or with County equipment is prohibited. Inappropriate use includes, but is not limited to, the following:

- Downloading, uploading, transmitting, or otherwise distributing any content that violates any existing laws, regulations, DBH policies, or personnel rules. This includes, but is not limited to, items that are:
  - Discriminatory;
  - Harassing or disruptive to other employees, including any sexually explicit, derogatory, abusive or threatening images cartoons, jokes, or other materials, unless any of the above is required for the performance of assigned job duties;
  - Copyrighted materials without proper permission or in violation of licensing agreements, and
  - Unapproved games.
- Participating in:
  - Chat room discussions or posting to electronic bulletin boards unless doing so is a function of DBH responsibilities, and
  - Any gambling, gaming or wagering activities.
- Downloading and using any software, scripting tools, or other mechanisms designed to monitor or disrupt DBH computing resources or subvert DBH security mechanisms;
- Using video and/or audio streaming and downloading technologies for non-DBH business purposes, and
- Personal use that results in any charges or other costs to DBH.

Monitoring Internet Usage

DBH reserves the right to monitor County provided Internet access and usage. Users of the Internet do so with the understanding that their usage may be monitored. No user should have an expectation of privacy in the use of the Internet through the County system or with County equipment.

Continued on next page

User Accounts and Passwords

Users must not share their DBH Internet accounts or passwords with others. Internet access will be granted to approved users and devices in accordance with the Information Technology Account Management Policy (IT5017). Approved users will be assigned access level based on their Internet Security and Acceleration (ISA) Proxy Group Placement by Job Classification.

Remote Access to Workstations and Servers

DBH has taken steps to ensure the security of the County's networks. These include the installation of security devices such as firewalls, monitoring systems, and other security measures. The following requirements apply to remotely accessing workstations and servers:

- Modems shall not be used to gain remote access to workstations and servers or to allow workstations and servers to make connections to other computers on the internal County network or outside the County's network.
- Computers outside the County's network that require access into the County's network may do so only through use of the County's secure Virtual Private Network (VPN).

Malware Protection

To protect DBH information resources, DBH IT must ensure malware protection software is employed and regular procedures are in place to ensure malware protection software is kept up to date. Desktop and laptop Computers that access the County network with a VPN must have appropriate malware protection software installed. Users may only access the Internet using County equipment if appropriate malware (e.g., virus, worm, spam) protection software has been installed by IT staff.

Consequences of Violations

Staff violating the use of DBH systems as defined in the prohibited activities section above or in other County policies may be subject to disciplinary action up to and including termination of employment.

Related Policy or Procedure

San Bernardino County Policy Manual:

- Internet/Intranet Use Policy (14-04)

DBH Standard Practice Manual and Forms:

- Computer and Network Appropriate Use Policy (IT5004)
- Remote Access Policy (IT5006)
- Device and Media Controls Policy (IT5008)
- User I.D. and Password Policy (IT5009)
- Information Technology Account Management Policy (IT5017)

References

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA); Security Rule.