County of San Bernardino
Department of Behavioral Health

Computer and Network Appropriate Use Policy

Effective Date 10/05/2006
Revision Date 10/26/2010

Allan Rawland, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) to utilize Behavioral Health and/or County electronic systems for legitimate department business purposes only.

Purpose

To provide DBH staff with information regarding the appropriate use of department systems also including those network services provided by the County.

Definitions

Non-Sanctioned Device can be defined as any equipment, software, application or electronic tools that have not been procured and/or approved by Information Technology (IT).

PHI is Protected Health Information.

PII is Personally Identifiable Information.

Staff/Users/Employees are interchangeable terms and will be used to reference DBH or other departmental employees, volunteers, work study individuals, contracted service personnel, vendors and others who have been authorized access to computers and/or computer lab facilities.

Systems is all inclusive and will be used to reference computers, workstations, desktops (physical and virtual), laptops, software applications, video-conferencing equipment, servers (physical and virtual), and networks or network services throughout this document.

General Information

County and/or department computer systems are provided to employees to assist them in the performance of their job duties. Using the systems for other than DBH business is prohibited.

Staff should have no expectation of privacy in anything they create, store, send or receive on a DBH system. All business conducted on departmental systems is considered the property of the department and therefore, open to view and/or monitoring by authorized personnel.

Continued on next page

Computer and Network Appropriate Use Policy, Continued

Information Technology Responsibilities

IT is responsible for:

- Issuing unique system User Identifications (User-I.D.)s and complex passwords, which allow users access to applications, networks and the Internet
- Protecting the data and information stored on all system servers and ensuring that such data is recoverable and restorable in the event of damage or loss, including the development of a business contingency plan
- Ensuring all County and department policies, Federal and State regulations and HIPAA Security Rules within its area of responsibility are maintained, monitored, and exceptions are properly documented and reported
- Controlling the rate of technology introduction and the types of technologies deployed within DBH
- Ensuring continued compliance with licensing laws

IT will randomly scan for inappropriate file types. Files will be purged from the system without prior staff notification, when inappropriate use is found.

Staff Responsibility

Staff has the responsibility to use system resources professionally, ethically and lawfully as further defined in County Policy 14-04 Internet/Intranet Use Policy and in the Internet Access Policy.

Staff is directly responsible for all actions resulting from the use of their User I.D. and password. User I.D. and password specifics are further defined in the User I.D. and Password Policy.

Examples of Violations

These acts include but are not limited to the following:

- Use of the Internet or system resources for reasons other than for DBH business purposes
- Download or store applications, system software, audio, video, or picture files to department systems unless these files are required to perform operational responsibilities

Users may not:

- Install or connect any non-sanctioned device onto DBH systems or the County's network
- Install custom screen savers on DBH systems without written approval from IT

Continued on next page

Computer and Network Appropriate Use Policy, Continued

Examples of Violations (continued)

- Store electronic data without receiving prior authorization from IT to include PHI and/or PII, on:
  - Diskettes
  - Computer Disks (CD)s
  - Recordable (DVDR) and DVD Rewriteable (DVDRW) disks
  - A systems hard drive (drive C)
  - External/portable hard drives
  - USB flash drives
  - Any other devices manufactured for this purpose

  Note: Any external/portable hard drive or USB flash drive issued by IT must have as a minimum, 256-Bit encryption.

- Remove or manipulate any authorized software placed on DBH systems by IT
- Copy operating systems, software or utility tools from a DBH system for use on home computers or for personal gain
- Modify, revise, transform, recast, adapt, reverse-engineer, disassemble or decompile any software
- Intentionally disrupt a network service
- Work on personal activities that incur additional cost to the department or interfere with a user's work performance
- Participate in chat room discussions, post or view electronic bulletin boards and social networking web-sites (Facebook, MySpace, etc.) unless doing so is a function of County responsibility
- Use video and/or audio streaming and downloading technologies for non-County purposes
- Download, upload, use or otherwise distribute copyrighted material without written permission or in violation of licensing agreements
- Use work time and resources for personal gain, personal services, advertisement, or personal for-profit business interests
- Post or send threatening or offensive messages
- Download, upload, transmit or otherwise distribute any content that violates any existing law, regulation, County policy, departmental or personnel rule
- Download, store, or send inappropriate e-mail or other forms of electronic communication that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or otherwise in violation of County policy

Continued on next page

Computer and Network Appropriate Use Policy, Continued

Consequences of Violations

Staff violating the use of DBH systems as defined above or in other County policies may be subject to disciplinary action including and up to termination of employment. Deliberately performing acts that waste system resources or unfairly monopolize resources to the exclusion of others may affect the level of recommended level of discipline.

References

Code of Federal Regulations 42, Part 431.300, Section 2.1 et seq.
Code of Federal Regulations 45, Parts 160 and 164.
California Civil Code 56 et seq. (The Confidentiality of Medical Information Act)
California Health and Safety Code (Information Practices Act of 1977), Section 1798
et seq., Section 123100 et seq. (Client Access to Health Records)
California Welfare and Institutions Code, Sections 5328 et seq., 14100
Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, Privacy Rule (HIPAA)
Department of Behavioral Health Medi-Cal Privacy and Security Agreement

Related Policy or Procedure

County Policy 14-01: Electronic Mail (E-mail) Policy
County Policy 14-04: Internet/Intranet Use Policy
County Policy 16-02: Protection of Individually Identifiable Health Information
County Policy 16-02SP1: Protections of Individually Identifiable Health Information
DBH Standard Practice Manual IT5003: Internet Access Policy
DBH Standard Practice Manual IT5005: Electronic Mail Policy
DBH Standard Practice Manual IT5006: Remote Access Policy
DBH Standard Practice Manual IT5008: Device and Media Controls Policy
DBH Standard Practice Manual IT5009: User I.D. and Password Policy