



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT <b>WORKSTATION USE AND SECURITY</b>	POLICY NO. <b>551.03</b>	EFFECTIVE DATE <b>04/20/2005</b>	PAGE <b>1 of 9</b>
APPROVED BY:  Director	SUPERSEDES <b>500.36 04/20/2005</b>	ORIGINAL ISSUE DATE <b>04/20/2005</b>	DISTRIBUTION LEVEL(S) <b>1</b>

**PURPOSE**

- 1.1 To restrict workstation use and access to Protected Health Information (PHI) and other confidential information by using physical, administrative, and technical controls.

**POLICY**

- 2.1 Los Angeles County Department of Mental Health (LACDMH) must ensure that workstation security procedures are enforced within each facility. "Workstations" include County and personal computers, mobile devices - e.g., tablet personal computers (PCs), personal digital assistants (PDAs), cellular telephones, computer carts - modems; printers, and fax machines, etc., that are used for County business.
  - 2.1.1 All users must use workstations in a manner commensurate with the sensitivity of the information accessed from the workstations.
    - 2.1.1.1 Access and Use of Workstation and Network Services
      - 2.1.1.1.1 Measures to limit unauthorized access must include the following:
        - 1. Configuration of workstation and network services.
          - a. System Managers/Owners must configure workstations and network services to allow only authorized access to the workstation and network services (e.g., data, applications, intranet, and internet).



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>WORKSTATION USE AND SECURITY</b>	<b>551.03</b>	<b>04/20/2005</b>	<b>2 of 9</b>

- b. Workforce Members must have both authorization to access a workstation and the appropriate rights to do so. Users must not access any confidential and/or sensitive information from a workstation unless they have authorization to do so, and it is necessary for doing their job.
- 2. Permitting only authorized access to workstations and network service through the use of controls.
  - 2.1.2 All users must take reasonable physical security precautions to prevent unauthorized physical access to sensitive information from workstations. These precautions include taking into consideration the physical attributes of the surroundings (e.g., concealing video displays and securing unattended workstations).
    - 2.1.2.1 Computer monitors must be positioned away from common areas, or a privacy screen must be installed to prevent unauthorized access or observation in accordance with LACDMH Policy 508.01, Safeguards for Protected Health Information.
  - 2.1.3 LACDMH Systems Managers/Owners must implement physical safeguards to permit only authorized user access to workstations with accessibility to confidential and/or sensitive information.
    - 2.1.3.1 General
      - 2.1.3.1.1 Workstations located in public or open areas must be physically secured in a locked room, secured in locked cabinets, or strongly anchored to deter unauthorized movement. Security cameras or additional forms of monitoring should be considered in high-risk areas.



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>WORKSTATION USE AND SECURITY</b>	<b>551.03</b>	<b>04/20/2005</b>	<b>3 of 9</b>

2.1.3.1.2 Workstations must be set up to generate a password-protected screen saver when the computer receives no input for a specified period of time (to be determined by the LACDMH Department Information Security Officer (DISO) based on the result of the risk assessment). The LACDMH Chief Information Officer (CIO) or his/her designee may approve other "lockout" schemes that protect against the unauthorized access to confidential and/or sensitive information.

2.1.3.1.3 Mobile devices must be secured when not in use. These devices must either be carried on persons or must be stored in secured areas.

2.1.3.1.4 Devices must be located in environments that are in accordance with the equipment manufacturer's operational specifications.

2.1.3.1.5 Inventory and maintenance records must be maintained for all workstations.

2.1.3.2 Physical Attributes of Surroundings

2.1.3.2.1 Workforce Members must be aware of the physical attributes of the surroundings where the workstation is located. Precautions need to be taken to prevent unauthorized access of unattended workstations, to automatically erase sensitive information left displayed on unattended workstations, and to limit the ability of an unauthorized individual to observe sensitive information when a workstation is in use by a user. The following measures must be taken:

1. Confidential data (e.g., patient information) must be password protected, encrypted, or stored on a secure network drive.



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

<b>SUBJECT</b>	<b>POLICY NO.</b>	<b>EFFECTIVE DATE</b>	<b>PAGE</b>
<b>WORKSTATION USE AND SECURITY</b>	<b>551.03</b>	<b>04/20/2005</b>	<b>4 of 9</b>

2. Confidential data having a Sensitivity Score of "High" must be encrypted.
3. Confidential data must not be downloaded without authorization from the LACDMH CIO or his/her designee.
4. Confidential data must not be saved on removable devices (e.g., floppy disk, Compact Disc Read Only Memory (CD-ROM), external drives; Universal Serial Bus (USB) drives) without proper safeguards and authorization from the LACDMH CIO or his/her designee. Removable media containing confidential data (e.g., patient information) must be maintained and stored in secured areas.
5. Printers are not to be left unattended in non-secure areas when printing confidential and/or sensitive information.
6. Disposal of confidential electronic records stored on removable or external media (e.g., CD-ROM, diskettes, hard drives) must be in accordance with LACDMH Policy No. 554.01, LACDMH Device and Media Controls.
7. Use caution when viewing and entering confidential information.
8. Layout and design of the space must shield the view of the workstation screen from the public, unless the requirements of No. 9, below, apply and are complied with.
9. Where it is not possible, through layout and design of the space, to shield the workstation



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>WORKSTATION USE AND SECURITY</b>	<b>551.03</b>	<b>04/20/2005</b>	<b>5 of 9</b>

screen from view, devices like privacy screens and shields are to be used.

2.1.3.3 Hardware/Software

2.1.3.3.1 Workforce Members must not change the system configuration of their workstation (e.g., network properties, video card) without proper authorization.

2.1.3.3.2 Workforce Members must not install or uninstall software (e.g., downloaded Internet software, games, patches, plug-ins, screen savers) on their workstation without proper authorization and licensing.

2.1.3.3.3 Only authorized users may install/uninstall software and perform repair services on workstations.

2.1.3.3.4 Workforce Members must not re-enable floppy drives, CD-ROM drives, USB ports, etc., on workstations that have access to confidential data, unless the Workforce Member is authorized to use those drives.

2.1.3.3.5 The Facility Manager/Program Head or his/her designee must ensure that appropriate controls are in place when sending equipment off premises for maintenance (i.e., the maintenance contract must include business associate language).

2.1.3.3.6 All hardware and software connected to a facility's network services must be managed centrally within each facility.

2.1.4 All users who use workstations as described above must be trained to exercise proper security practices. Training and documentation must be in accordance with the LACDMH Privacy and Security Compliance



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>WORKSTATION USE AND SECURITY</b>	<b>551.03</b>	<b>04/20/2005</b>	<b>6 of 9</b>

Program policies and procedures, including LACDMH Policy No. 553.01, Privacy and Security Awareness and Training, and LACDMH Policy No. 555.01, LACDMH Data Security Documentation Requirement.

#### 2.1.4.1 Unique User ID's and Passwords

2.1.4.1.1 The LACDMH DISO or his/her designee is responsible for ensuring the assignment of a unique User ID or each user, to identify and track the user's identity when logging into workstations, networks, or applications.

2.1.4.1.2 Each user must protect his/her password. Users must not write down their password and place it at or near the workstation (e.g., a note taped to the monitor or placed under the keyboard).

2.1.4.1.3 Logging into workstations, networks, or applications with another user's ID and/or password is prohibited.

2.1.4.1.4 Users must not share their unique User IDs (logon/system identifier) with any other person.

2.1.4.1.5 Users' passwords must be changed at least every ninety (90) days.

2.1.4.1.6 Passwords must be a least eight (8) characters long and contain a combination of alpha and numeric characters. The password may also include special characters.

2.1.4.1.7 Two-factor authentication in which the user provides two means of identification, one typically a physical token (e.g., a card) and the other typically something memorized, (e.g., a security code) must



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>WORKSTATION USE AND SECURITY</b>	<b>551.03</b>	<b>04/20/2005</b>	<b>7 of 9</b>

be used for information systems receiving a Risk Analysis Sensitivity score on "High."

(Refer to LACDMH Policy No. 550.01, LACDMH Security Management Process: LACDMH Risk Management to determine the Risk Analysis Sensitivity Score.)

2.1.4.2 Other User Authentication Methods

2.1.4.2.1 With authorization from the LACDMH DISO may utilize other user authentication methods (e.g., badge readers, biometric devices, tokens).

2.1.4.3 Access to Workstations Not in Use

2.1.4.3.1 Workstations not in use must be password protected and locked.

2.1.4.3.2 Workstations must be set up to generate a password-protected screen saver when the computer receives no input for a specified period of time (to be determined by the LACDMH CIO based on the result of the risk assessment). The LACDMH CIO or his/her designee may approve other "lockout" schemes that protect against the unauthorized access to confidential and/or sensitive information.

2.1.4.4 Workstations must display an appropriate warning banner prior to gaining operating systems access.

2.1.4.5 Access and Use of Mobile Devices

2.1.4.5.1 Mobile devices must be pre-approved and registered for use in a facility by the LACDMH CIO or his/her designee.



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>WORKSTATION USE AND SECURITY</b>	<b>551.03</b>	<b>04/20/2005</b>	<b>8 of 9</b>

2.1.4.5.2 Workforce Members must exercise good judgment in determining the amount of necessary data stored on their mobile devices to perform their functions.

2.1.4.5.3 Access to mobile devices must be protected at all times consistent with the procedures set forth in Attachment 1, Workstation Use and Security Procedures, and Access and Use of Workstation and Network Services section above.

2.1.4.5.4 Mobile devices containing sensitive information (e.g., confidential patient information) must be encrypted.

2.1.4.5.5 When traveling, a Workforce Member must not leave mobile devices unattended in non-secure areas.

2.1.4.5.6 Mobile devices that are left in cars must be stored out of sight, and the car must be locked.

**DEFINITIONS**

3.1 Workforce Member: Employees, volunteers, trainees, and other persons under the direct control of Los Angeles County, whether or not they are paid by Los Angeles County.

3.2 Protected Health Information (PHI): Individually identifiable information relating to (1) past, present, and future physical or mental health or condition of an individual; (2) provision of health care to an individual; or (3) the past, present, or future payment for health care provided to an individual.

3.3 System Managers/Owners: The person who is responsible for the operation and use of a system.



## DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>WORKSTATION USE AND SECURITY</b>	<b>551.03</b>	<b>04/20/2005</b>	<b>9 of 9</b>

For a more complete definition of terms used in this policy and/or procedure, see the LACDMH Information Security Glossary, Attachment 1 of LACDMH Policy No. 555.02, LACDMH Information and Technology Security.

### **AUTHORITY**

1. **MANDATED BY** 45 Code of Federal Regulations, Part 164, Subpart C, Section 164.310(a)(2)(iv)(b) and (c)
2. Board of Supervisors Policies:
  - 6.100, Information Technology and Security Policy
  - 6.102, Countywide Antivirus Security Policy
  - 6.106, Physical Security

### **CROSS REFERENCES**

Administrative Controls:

LACDMH Policy No. 550.02, Workforce Members Security

Technical Controls:

LACDMH Policy No. 554.02, System Access Control

LACDMH Policies:

508.01, Safeguards for Protected Health Information  
550.01, Security Management Process: LACDMH Risk Management  
553.01, Privacy and Security Awareness and Training  
554.01, LACDMH Device and Media Controls  
555.01, LACDMH Data Security Documentation Requirement

### **ATTACHMENT (HYPERLINKED)**

1. [Workstation Use and Security Procedures](#)

### **REVIEW DATE**

This policy shall be reviewed on or before January 2010.