LOS ANGELES COUNTY
DEPARTMENT OF MENTAL HEALTH

Policy Title: **Workstation Use and Security**
Policy Number: 551.03
Policy Category: Administrative
Distribution Level: Directly-Operated Programs and Contracted Agencies
Responsible Party: Chief Information Office Bureau

I. POLICY STATEMENT

The purpose of this policy is to restrict access to sensitive and confidential information such as Protected Health Information (PHI) to only authorized DMH workforce members by using physical, administrative, and technical safeguards on all computing devices.

Contracted agencies shall develop an internal policy and associated procedures that are consistent with their organizational practices and meet the requirements set forth in this policy.

II. DEFINITIONS

Terms used within this policy are defined in the DMH Information Technology and Security Glossary.

III. POLICY

Los Angeles County Department of Mental Health (DMH/Department) must ensure workstation security procedures are strictly enforced within each facility to maximize the protection of PHI.

All workstations must be used in a manner commensurate with the sensitivity of the information accessed via those workstations.

Only DMH-issued equipment shall be connected to the County network. DMH-issued equipment shall only be used to conduct County business and store County data.

All workforce members must take reasonable physical security precautions to prevent unauthorized physical access to sensitive information from workstations. Physical attributes of surroundings must be taken into consideration (e.g., concealing screen displays and securing unattended workstations).

- Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized observation or access in accordance with DMH Policy 508.01.
- Computer peripherals such as network printers and fax machines must not reside in crowded common areas or public spaces.

Policy Title: **Workstation Use and Security**
Policy Number: 551.03

DMH systems managers/owners must implement physical safeguards to permit only authorized user access to workstations with accessibility to confidential and/or sensitive information.

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 DMH Policies 553.01 and 555.01.

IV. PROCEDURES

Click here to view procedures.

V. AUTHORITY

Board of Supervisors Policy No. 6.100, Information Security Policy
Board of Supervisors Policy No. 6.101, Use of County Information Assets
Board of Supervisors Policy No. 6.102, Endpoint Security Policy
Board of Supervisors Policy No. 6.103, Information Security Incident Reporting
Board of Supervisors Policy No. 6.104, Information Classification Policy
Board of Supervisors Policy No. 6.105, Information Technology Audit and Risk Assessment Policy
Center for Medicare & Medicaid Services (CMS) HIPAA Security Series 3: Physical Safeguards
Code of Federal Regulations Title 45 Section 164.310(a)(2)(iv), Maintenance records
Code of Federal Regulations Title 45 Section 164.310(b), Standard: Workstation use

VI. ATTACHMENTS

DMH Information Technology and Security Glossary

VII. EFFECTIVE DATES

This policy was effective April 20, 2005.

Review Date: May 28, 2019 Reviewed with Revisions

VIII. SIGNATURE, TITLE, and DATE OF APPROVAL

Required for initial approvals and all subsequent reviews and updates.

Name/Title

6/5/19
Date