



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT SYSTEM ACCESS CONTROL POLICY	POLICY NO. 554.02	EFFECTIVE DATE 04/20/2005	PAGE 1 of 5
APPROVED BY:  Director	SUPERSEDES 500.43 04/20/2005	ORIGINAL ISSUE DATE 04/20/2005	DISTRIBUTION LEVEL(S) 1

PURPOSE

1.1 This policy states the technical security requirements for electronic information systems to allow access only to persons or software programs that have appropriate access rights.

POLICY

2.1 The Los Angeles County Department of Mental Health (LACDMH) Chief Information Officer (CIO) must ensure that the System Managers/Owners implement the appropriate access control safeguards to allow LACDMH electronic information systems access only to those persons or software programs who have been granted access rights:

- 2.1.1 Unique user identification. LACDMH systems must assign a unique name and/or number for identifying and tracking user identity.
- 2.1.2 System Login Banner. Every login process for multi-user computers must include a special notice as contained in the procedure section (Attachment 1).
- 2.1.3 System Login Monitoring. User and process access to system must be recorded and monitored for successful and failed attempts.
- 2.1.4 Emergency Access Procedure. LACDMH electronic systems must have alternate secured manual or automated procedures for accessing stored information during an emergency invoked by the Departmental Information Security Officer (DISO) or designee where the usual means of secured access is not available.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SYSTEM ACCESS CONTROL POLICY	554.02	04/20/2005	2 of 5

- 2.1.5 Automatic logoff. LACDMH must be sure to address the use of an automated process to terminate an electronic session after a predetermined time of inactivity.
 - 2.1.6 Encryption/Decryption. LACDMH must ensure that the System Managers/Owners addresses the appropriate encryption for protecting electronic information contained within the storage structure for all LACDMH electronic data storage systems (i.e., databases or file systems) based on the LACDMH Master Security Management Report in the LACDMH Policy 550.01, Security Management Process: LACDMH Risk Management.
 - 2.1.7 Information system access control review and documentation. The DISO, taking into consideration each system's Risk Analysis Sensitivity Score, must approve the design and implementation of controls to limit unauthorized access of Workforce Members to information systems, including workstations, servers, networks, and applications.
- 2.2 The System Managers/Owners must document the implementation of the above safeguards in the System Security Documentation that accompanies the electronic data system. The system security documentation and all system documentation must be submitted to the DISO or designee for review.

DEFINITIONS

- 3.1 System Security Documentation: The system security documentation describes the strategy for security and addresses the security measures and program safeguards which will ensure that information systems and resources:
 - a. Operate effectively and accurately;
 - b. Are protected from unauthorized alteration, disclosure, or misuse of information processed, stored, or transmitted;
 - c. Can maintain the continuity of automated information support for the entity missions, programs, and function;



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
SYSTEM ACCESS CONTROL POLICY	554.02	04/20/2005	3 of 5

- d. Incorporate management, general, and application controls sufficient to provide cost-effective assurance of the system's integrity and accuracy; and
- e. Have appropriate technical, personnel, administrative, environmental, and access safeguards.

System security documentation is a system and component level documentation that describes the system security requirement and how it has been implemented. At the component level, documentation includes operating system documentation, the security system documentation, and application documentation. At the system level, security documentation includes interrelationships among applications and with the operating system and utilities in its environment.

The system security documentation includes, but is not limited to, creation and maintenance of the following documents:

- Design Documentation Report. This report provides a description of the developer or integrator's philosophy of protection and an explanation of how this philosophy is translated in the system. The report describes how the security strategy was implemented. This can also include description of a security policy model and an explanation of how the system enforces the security policy.
- Test Documentation Report. A report that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing.
- Security Features User's Guide. A system- and product-level documentation that describes the protection mechanisms provided by the system,



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT SYSTEM ACCESS CONTROL POLICY	POLICY NO. 554.02	EFFECTIVE DATE 04/20/2005	PAGE 4 of 5
---	------------------------------------	--	------------------------------

guidelines on their use, and how they interact with one another.

- System Administrator Manual. A system- and component-level manual that provides guidance to the system administrator and presents cautions about functions and privileges that should be controlled when running the system or facility in a secure manner. This guidance includes procedures for examining and maintaining security features (such as audit record structures). The manual should describe the operator and administrator functions related to security, including changing the security characteristics of a user. It should provide guidelines on the consistent and effective use of the protection features of the system, how they interact, warnings, and privileges that need to be controlled in order to operate the system or facility in a secure manner.

The System Security Documentation is part of the system compliance documentation mentioned in DMH Policy No. 555.01, LACDMH Data Security Documentation Requirement Policy.

3.2 System Managers/Owner: The person who is responsible for the operation and use of a system

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

PROCEDURE

4.1 Follow the procedures detailed in Attachment 1.



**LAC
DMH**
LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH

**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT SYSTEM ACCESS CONTROL POLICY	POLICY NO. 554.02	EFFECTIVE DATE 04/20/2005	PAGE 5 of 5
---	------------------------------	--	------------------------

AUTHORITY

MANDATED BY 45 Code of Federal Regulations, Part 164, Subpart C,
Section 164.308 (a)(3)(ii)

ATTACHMENT (HYPERLINKED)

1. [System Access Control Procedures](#)

REVIEW DATE

This policy shall be reviewed on or before January 2010.