



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT <b>SECURITY MANAGEMENT PROCESS: LACDMH RISK MANAGEMENT</b>	POLICY NO. <b>550.01</b>	EFFECTIVE DATE <b>04/20/2005</b>	PAGE <b>1 of 5</b>
APPROVED BY:  Director	SUPERSEDES <b>500.29 04/20/2005</b>	ORIGINAL ISSUE DATE <b>04/20/2005</b>	DISTRIBUTION LEVEL(S) <b>1</b>

**PURPOSE**

- 1.1 To create and implement security management processes that ensure the security (confidentiality, integrity, and availability) of Protected Health Information (PHI) and other confidential information.

**POLICY**

- 2.1 Los Angeles County Department of Mental Health (LACDMH) must establish and maintain a Security Management Process. The process must include, at minimum, a risk analysis of electronic data resources and information systems, including administrative, physical, and technical risks that could impact PHI and other confidential data; a risk management plan; an information systems activity review procedure; and application of a disciplinary action/sanction policy against workforce members and other users who fail to comply with the LACDMH Policy No. 553.02, LACDMH Privacy and Security Compliance Program.
- 2.2 Fundamental to this process is the availability of current LACDMH application and system inventories to ensure that all known systems will undergo risk assessment and have in place a risk management plan and activity review procedure. LACDMH must maintain an up-to-date inventory of all known applications and systems. The Security Management Process must also identify accountability. The Process must be documented and auditable.
  - 2.2.1 Risk Analysis

LACDMH must ensure that System Managers/Owners conduct risk assessments for their data resources and information systems. LACDMH must document their risk assessment results in a Risk Analysis Report. The Risk Analysis Report must be provided to the



# DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>SECURITY MANAGEMENT PROCESS: LACDMH RISK MANAGEMENT</b>	<b>550.01</b>	<b>04/20/2005</b>	<b>2 of 5</b>

LACDMH Department Information Security Officer (DISO) or his/her designee for review and approval.

### 2.2.2 Risk Management

A LACDMH Master Security Management Report must be created by the Los Angeles County Department of Mental Health Chief Information Officer (LACDMH CIO) or his/her designee and updated periodically to identify system and application risks and to recommend safeguards and actions to mitigate those identified risks. The recommended safeguards and actions must expressly include justifications for any decision to not mitigate system or application risk.

LACDMH must develop appropriate plans to implement the Master Security Management Report's recommended safeguards and actions.

The LACDMH Master Security Management Report and mitigation plans must be provided to the DISO or his/her designee for review and approval. The reports must be kept confidential and the information released only to those with a need to know in order to remediate or supervise remediation.

### 2.2.3 Disciplinary Action/Sanction Policy

LACDMH workforce members who violate any LACDMH data security policies and procedures are subject to discipline in accordance with the administrative specification in LACDMH Policy No. 605.01, Discipline; Civil Service Rule 18.031; and the LACDMH Employee Reference Manual.

Non-LACDMH County workforce members, contractors, and agencies that violate the security policies and procedures are subject to sanctions or penalties imposed pursuant to the applicable contract or memorandum of understanding (MOU) and/or Federal, State, or local law.



SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>SECURITY MANAGEMENT PROCESS: LACDMH RISK MANAGEMENT</b>	<b>550.01</b>	<b>04/20/2005</b>	<b>3 of 5</b>

2.2.4 Information Systems Activity Review

LACDMH must establish, document, and implement procedures and schedules for reviewing information systems activity, including, but not limited to, audit logs, problem logs, system access reports, change control logs, and security incident reports.

2.2.5 LACDMH must conduct an evaluation of its security safeguards annually, or more frequently when there are changes in the LACDMH security environment, to demonstrate and document compliance with both the County and LACDMH security policies and procedures

**DEFINITIONS**

3.1 LACDMH CIO The Los Angeles County Department of Mental Health Chief Information Officer

3.2 Risk The potential for harm or loss. Risk is best expressed as the answers to these four questions:

2. What could happen? (What is the threat?)
3. How bad could it be? (What is the impact or consequence?)
4. How often might it happen? (What is the frequency?)
5. How certain are the answers to the first three questions? (What is the degree of confidence?)

The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no "risk" per se.

3.3 Risk Assessment The identification and study of the vulnerability of a system and the possible threats to its security.



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>SECURITY MANAGEMENT PROCESS: LACDMH RISK MANAGEMENT</b>	<b>550.01</b>	<b>04/20/2005</b>	<b>4 of 5</b>

- 3.4 Risk Management The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.
- 3.5 System/Managers/Owners The person who is responsible for the operation and use of a system.
- 3.6 Threat An entity or event with the potential to harm the system. Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers, and viruses.
- 3.7 Vulnerability A condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat.
- 3.8 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.

For a more complete definition of terms used in this policy, refer to Policy No. 555.02, Information and Technology Security.

For additional information on this matter, please consult with the DISO.

**AUTHORITY**

- MANDATED BY** 45 Code of Federal Regulations (CFR) Part 164, §164.308(1)(i) Health Insurance Portability and Accountability Act (HIPAA) of 1986, 42 U.S.C. Sections 1320-d -1320-d-8
- Civil Service Rule 18.301



**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>SECURITY MANAGEMENT PROCESS: LACDMH RISK MANAGEMENT</b>	<b>550.01</b>	<b>04/20/2005</b>	<b>5 of 5</b>

3. LACDMH Employee Reference Manual

**ATTACHMENT (HYPERLINKED)**

1. [Security Risk Management Procedures](#)

**REVIEW DATE**

This policy shall be reviewed on or before January 2010.

**RESPONSIBLE PARTY**

LACDMH Chief of Information Bureau