




**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT <b>SECURITY INCIDENT REPORT AND RESPONSE</b>	POLICY NO. <b>552.01</b>	EFFECTIVE DATE <b>04/20/2005</b>	PAGE <b>1 of 2</b>
APPROVED BY:  Director	SUPERSEDES <b>500.32 04/20/2005</b>	ORIGINAL ISSUE DATE <b>04/20/2005</b>	DISTRIBUTION LEVEL(S) <b>1</b>

**PURPOSE**

- 1.1 To develop, implement, and maintain appropriate security incident identification, response, mitigation, and related documentation processes.

**POLICY**

- 2.1 The Los Angeles County Department of Mental Health (LACDMH) Workforce Member must immediately report any and all suspected and actual breaches of information security to his/her supervisor and then to the LACDMH Help Desk or Departmental Information Security Office (DISO). The DISO will activate the Departmental Computer Emergency Response Team (DCERT), and a DCERT Representative must ensure notification of all other DMH sites and/or persons - (e.g., LACDMH Chief Information Officer (CIO), System Managers/Owners) - of computer security threat events. The DCERT Representative must also notify the Privacy Officer if the security incident involves Protected Health Information.
- 2.2 The DISO or DCERT Representative is responsible for determining the appropriate level of response to a security incident and who outside of LACDMH needs to be notified.
- 2.3 The LACDMH security incident reporting response procedures, including the Incident Report form, must be consistent with the County Security Incident Report and Response policies and procedures.

**DEFINITIONS**

- 3.1 CCERT: Countywide Computer Emergency Response Team. CCERT has responsibility for response and reporting of information technology (IT) security incidents.



DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>SECURITY INCIDENT REPORT AND RESPONSE</b>	<b>552.01</b>	<b>04/20/2005</b>	<b>2 of 2</b>

- 3.2 CERT: Computer Emergency Response Team. CERT has responsibility for response and reporting of IT security incidents within an organization.
- 3.3 DCERT: Departmental Computer Emergency Response Team. DCERT has responsibility for response and reporting of IT security incidents.
- 3.4 Incident: An occurrence or event that interrupts normal procedure or precipitates a crisis.
- 3.5 System Managers/Owners: 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 Technology and Security.

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

**AUTHORITY**

- 1. **MANDATED BY** 45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.308(a)(6)(i)
- 2. Board of Supervisors Policy No. 6.103, Countywide Computer Security Threat Responses

**ATTACHMENT (HYPERLINKED)**

- 1. [Security Incident Report and Response Procedures](#)

**REVIEW DATE**



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

**DEPARTMENT OF MENTAL HEALTH  
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
<b>SECURITY INCIDENT REPORT AND RESPONSE</b>	<b>552.01</b>	<b>04/20/2005</b>	<b>3 of 2</b>

This policy shall be reviewed on or before January 2010.