



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT INFORMATION TECHNOLOGY CONTINGENCY PLAN	POLICY NO. 550.03	EFFECTIVE DATE 04/20/2005	PAGE 1 of 3
APPROVED BY:  Director	SUPERSEDES 500.33 04/20/2005	ORIGINAL ISSUE DATE 04/20/2005	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To define the Los Angeles County Department of Mental Health (LACDMH) Information Technology (IT) Contingency Plan.

OVERVIEW

- 2.1 LACDMH must ensure the security (confidentiality, integrity, and availability) of Protected Health Information (PHI) and other confidential information in the event of any disruption, disaster, or other emergency by planning for the recovery and continued operation of electronic information systems.
- 2.2 Underlying the entire IT Contingency Plan is the criticality analysis and the data backup plan. While the criticality analysis identifies the relative importance of LACDMH's information systems, the data backup plan ensures that the necessary data and the right amount of data are retrievably stored off site on a pre-determined schedule.
- 2.3 In accordance with the priority determined in the criticality analysis, the disaster recovery plan focuses on the sequence and method of recovering information systems, and the data they hold, from the data secured in storage by the backup plan. In contrast, the emergency mode operation plan assures the day-to-day operations during the emergency with the minimum required data set, with or without a full recovery of the system.

POLICY

- 3.1 LACDMH must develop and implement an IT Contingency Plan. The IT Contingency Plan serves as a master plan for responding to IT system emergencies (e.g., fire, vandalism, system failure, and natural disaster) ensuring continuity of operation during an emergency and recovery from a disaster. The IT Contingency Plan shall include:



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION TECHNOLOGY CONTINGENCY PLAN	550.03	04/20/2005	2 of 3

- 3.1.1 Policies and procedures that address electronically maintained or transmitted PHI and other information.
- 3.1.2 Applications and Data Criticality Analysis - an assessment of the relative criticality of specific electronic information systems and data.
- 3.1.3 Data backup - a process for retrieving exact copies of data.
- 3.1.4 Disaster recovery - procedures for restoring any lost data.
- 3.1.5 Emergency mode of operations - procedures to enable business continuity and protect the security of electronic IT information during and immediately after an emergency.
- 3.1.6 Command and control - the provision of IT administrative direction in the event an emergency occurs.
- 3.1.7 Testing and revision procedures - procedures for performing periodic testing and revision of the IT Contingency Plan.
- 3.1.8 Workforce IT Contingency Plan training - training and preparation of designated Workforce Members regarding the IT Contingency Plan.
- 3.2 The Contingency Plan will be tested as set forth as outlined in Testing and Revision of Contingency Plan of the procedures (Attachments 1 through 8), at least once every year and updated as necessary.
- 3.3 The Departmental Information Security Officer is responsible for reviewing and updating the IT Contingency Plan. IT Contingency Plans may be periodically enhanced as appropriate to further LACDMH's business purposes. All IT Contingency Plans including the components identified in paragraphs 3.1.1 through 3.1.8 above and any revisions must be provided to the Chief Information Officer for review and approval.

DEFINITIONS

- 4.1 Contingency Plan: A plan for emergency response, backup procedures, and post-disaster recovery, synonymous with disaster plan and emergency plan.



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
INFORMATION TECHNOLOGY CONTINGENCY PLAN	550.03	04/20/2005	3 of 3

4.2 Disaster Recovery: A plan for the restoration of lost data, or the reconciliation of conflicting or erroneous data, after a system failure due to natural or manmade disaster.

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, Information and Technology Security.

AUTHORITY

1. **MANDATED BY** 45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.308(a)(7)(i) and (ii)
2. Board of Supervisors Policies:
 - 6.100, Information Technology and Security Policy
 - 6.103, Countywide Computer Security Threat Response
 - 6.107, Information Technology Risk Assessment

ATTACHMENTS (HYPERLINKED)

1. [LACDMH Facility Information Technology Contingency Plan Procedures](#)
2. [Application and Data Criticality Analysis](#)
3. [Data Backup Plan](#)
4. [Disaster Recovery Plan](#)
5. [Emergency Mode Operation Plan](#)
6. [Command and Control Plan](#)
7. [Testing and Revision of Contingency Plan](#)
8. [Workforce Contingency Plan Training](#)

CROSS-REFERENCE

LACDMH Policy No. 550.01, Security Management Process: LACDMH Risk Management

REVIEW DATE

This policy shall be reviewed on or before January 2010.