RANCHO

Rancho Los Amigos National Rehabilitation Center
INFORMATION MANAGEMENT SERVICES
POLICY AND PROCEDURE

SUBJECT:	DISASTER RECOVERY AND CONTINGENCY PLANS	Policy No.:	207
		Supersedes:	207 (6/15/00)
		Revision Date:	9/21/06)
		Page:	1of 5

I. PURPOSE:

To establish guidelines for Information Management Services (IMS) in preparing all facility information systems in the event of any disaster or other emergency, and to provide a plan for the recovery from these disasters and continued operation of electronic information systems.

II. POLICY:

To organize Rancho Los Amigos National Rehabilitation Center's (RLANRC) resources in the event of an emergency, and to establish methods of dealing with disasters.

III. SUMMARY

The Disaster Recovery/Contingency Plan set forth by IMS at RLANRC contains the policies, scope, responsibilities, preparations and procedures necessary to meet the results of a disaster, such as an earthquake, fire, explosion, flood or any other disturbance that renders the data center partially or completely inoperative. The plan is arranged to cover two major functions:

- Disaster preparation policies and procedures
- Disaster recovery policies and procedures

The Data Center Disaster Recovery Coordinator administers and coordinates the plan. It is the Coordinator's responsibility to assure that all parties impacted by this plan are properly trained and knowledgeable of the plan and their specific tasks. It is also the responsibility of the Coordinator to administer and coordinate the recovery operation.

The disaster recovery team assumes the responsibility for this plan in the event of a disaster. The team consists of key individuals from the hospital administration, IMS and the facility end-user units. The team provides, first and foremost, for the protection and safety of personnel; secondly, for the protection of property; and thirdly, for the continuation of data center operations.

A. The IT Disaster Recovery and Contingency Plans serve 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 includes:

1. Policies and procedures that address electronically maintained or transmitted Protected Health Information (PHI) and other information.

2. Application and Data Criticality Analysis -an assessment of the relative criticality of specific electronic information systems and data.

3. Data backup – a process for retrieving exact copies of data.

4. Disaster recovery – procedure for restoring any lost data.

APPROVED BY:
Signature(s) on File.

5. Emergency mode of operations – procedures to enable business continuity and protect the security of **electronic IT information**-during and immediately after an emergency.

6. Command and control -the provision of IT administrative direction in the event an emergency occurs.

7. Testing and revision procedures- to perform periodic testing and revision of the IT Contingency Plan.

8. Workforce IT Contingency Plan training -to train and prepare designated **workforce members** regarding the IT Contingency Plan.

B. The Contingency Plan will be tested as set forth in paragraph VI. of the procedure below, Testing and Revision of Contingency Plan at least once every year and updated as necessary.

C. The DHS Facility CIO/designee is responsible for reviewing and updating the IT Contingency Plan. IT Contingency Plans may be periodically enhanced as appropriate to further DHS' business purposes. All IT Contingency Plans, and any revisions, must be provided to the facility departmental information security coordinator or CIO-delegate for review and approval to ensure that the minimum IT Contingency Plan requirements are met.

DEFINITIONS: CONTINGENCY PLAN A plan for emergency response, backup procedures, and post-disaster recovery. Definition is synonymous with disaster plan and emergency plan.

DISASTER RECOVERY PLAN 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.

INFORMATION TECHNOLOGY (IT) A term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, personal health information, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).

For a more complete definition of terms used in this policy and/or procedure, see the DHS Information Security Glossary, Attachment I to DHS Policy No. 935.00, DHS Information Technology and Security Policy.

IV. PROCEDURE: (Refer to the Disaster Recovery and Contingency Plan on file in IMS.)

A. Application and Data Criticality Analysis

The Application and Data Criticality Analysis must identify IT Contingency Plan priorities based on the criticality and sensitivity of the applications and data within RLANRC. The Application and Data Criticality Analysis includes:

1. Identification of the assets (e.g., hardware, software, and applications) utilized by the Facility that receive, manipulate, store and/or transmit confidential information, as well as information necessary to ongoing business operations.

2. Prioritization of applications and data based on the Criticality Score and Sensitivity Score found in the Facility Master Security Management Report, DHS Policy No. 935.01, Security Management Process: Risk Management.

B. Data Backup Plan

The Data Backup Plan must ensure that exact copies of critical data are retrievable. The Data Backup Plan must include the following steps:

1. Identify the backup methods (e.g., full, incremental, or differential backup) and materials (e.g., CD-ROM, magnetic tape, or floppy disks) to be used, and the frequency of performing backups based on the criticality analysis.

2. Assign a responsible person(s) to manually backup the data sets as determined, or configure the backups to be done automatically by available tools. The backups will be inspected and tested to ensure that their contents are exact copies of the data archived, and that they are restorable.

3. Assign a responsible person(s) to catalogue, store and secure the backups in a suitable container and location for such purpose.

4. Monitor and track storage and removal of backups; ensure all applicable access controls are enforced.

5. Track the archive requirements for each backed up data set; ensure they are maintained for the appropriate time period.

6. Test the Data Backup plan as set forth in the plan (or section F. below).

   Note: See IMS Policy Number 209 (Back-Up Procedure for File Servers) for the detailed back-up procedure.

C. The Disaster Recovery Plan must enable the restoration of lost data in the event of fire, vandalism, systems failure or other disaster. The Disaster Recovery Plan includes the following steps:

1. Assign and provide access rights to an authorized person(s) for the retrieval, loading and testing of data backups.

2. Retrieval of the latest copy of the Facility's backed up data from the secure location in the event of data loss. If the necessary data set(s) have not been archived, efforts will be made through formal channels (e.g., retransmission from original sources) to collect the data.

3. Load the retrieved data in the order of pre-determined criticality (especially with regard to the availability attribute), to appropriate components (in accordance with applicable access control policies) and test to ensure the data restoration was successful.

4. Test the Disaster Recovery plan as set forth in the plan.

D. Emergency Mode Operation Plan

The Emergency Mode Operation plan must enable the Facility to continue its operations and business processes in the event of fire, vandalism, systems failure or other disaster and safeguards the security of data. The Emergency Mode Operation Plan must be based on the criticality analysis for each IT Information System and must include the following steps:

1. Identify the scope including the severity of the emergency (e.g., system only, Facility-wide, DHS-wide) and the duration of the emergency (e.g., until repair, day, week, month, undetermined).

2. Identify type of recovery (e.g., hot site, warm site, cold site, disk mirroring) that is required by the scope of the emergency.

   Note: the cost of establishing a "hot site" is beyond the scope of the facility's budget. The facility has asked Los Angeles County Department of Health Services to provide a hot site for them. It is the hope that someday, there will be a hot site available. Until then, our "warm site" consists of our Affinity report server, located at Harbor-UCLA Medical Center.

3. Identify emergency continuity personnel including either backup personnel or personnel cross-trained to assure adequate staffing in the event of an emergency.

4. Designate specific roles and responsibilities to initiate and maintain emergency mode operations including information system and security personnel.

5. Implement the following emergency access control requirements:

   a. Determine emergency access control requirements for emergency mode operations in accordance with the Emergency Access Control Procedure in DHS Policy No. 935.14, System Access Control.

   b. Give Users additional privileges in the event of a crisis situation to access information as needed and in accordance with the above emergency mode operation procedures.

6. Test the emergency mode operation procedures as set forth in the plan (or section F. below).

E. Command and Control Plan

The Command and Control Plan must establish IT administrative procedures to follow in the event that an emergency occurs.

1. The DHS Facility CIO/designee must integrate the DHS Facility IT Contingency Plan with existing DHS Facility Contingency Plan to establish command and control in order to support emergency management team members who can facilitate the flow of information as necessary to users.

2. Develop a call tree to disseminate important information within DHS and/or the DHS Facility, as necessary.

3. Each DHS Facility must have in place a notification process to notify the appropriate persons within DHS and the DHS Facility. in the event any part of the IT Contingency Plan is executed.

F. Testing and Revision of Contingency Plan

The IT Contingency Plan must be tested periodically in order to assure the workability of the Plan in the event of a disaster and/or emergency. If testing establishes the need for changes in existing IT Contingency Plan procedures then those procedures must be revised.

1. Conduct one or more of the following exercises to test the IT Contingency Plan (including backup, disaster recovery, and emergency mode operation plans):

   a. Tabletop exercise of response to specific scenarios

b. Technical restoration activities

c. Supplier and/or services tests

d. Complete drills of the data backup plan, disaster recovery plan and the emergency mode operations plan.

2. Revise the IT Contingency Plan to address any deficiencies discovered during the testing activities. Focus on improvements to role and responsibility definitions, processes, practices, and strategies.

3. Revise the IT Contingency Plan as needed, if there are important changes involving personnel, contact information, suppliers, legislation, business risks, processes or strategies.

4. Annually conduct one or more of the exercises to test the IT Contingency Plan as set forth in paragraph A. above or when there are significant changes to the environment.

G. Workforce Contingency Plan Training

DHS facilities must train and prepare designated workforce members as necessary regarding the IT Contingency Plan.

AUTHORITY: 45 Code of Federal Regulations (CFR), Part 164, Subpart C, Section 164.308(a)(7)(i) and (ii)

Board of Supervisors Policies:
6.100, Information Technology and Security Policy
6.103, Countywide Computer Security Threat Response
6.107, Information Technology Risk Assessment

CROSS REFERENCE:
DHS Policy No. 935.01, Security Management Process: Risk Management
DHS Policy No. 935.14, System Access Control
RLANRC IMS Policy No. 209, Back-Up Procedure for File Servers