CSB
Policy And Procedures

MIS Disaster Recovery Plan

Policy Statement

The equipment, software systems, and databases that comprise the ePHI System are critical components that enable the [CSB] to function in an effective manner. The purpose of this plan is to provide the framework for recovering from any disaster that might affect these systems, to minimize downtime, and to assist users in meeting their critical processing requirements.

HIPA Security Regulations Addressed In This Policy

164.308(a)(7) Disaster Recovery Plan

References

Department of Mental Health, Mental Retardation, and Substance Abuse Administrative - MIS Data Backup and Storage Policy #20

Attachments

Attachment A (Disaster Recovery Team), B (Items for Complete System Recovery), C (System Requirements)

Implementation And Responsibility:

A. The decision to implement disaster recovery procedures is the responsibility of the MIS Director or his/her designee. The Disaster Recover Team, see Attachment A, will convene as soon as possible after a disaster has occurred to assess damages and make recommendations to the MIS Director.
B. This plan is distributed by the LAN Manager to and used by those persons responsible for its implementation and operation. These individuals are identified in Attachment A, Disaster Recovery Team Members. This document will be maintained and updated by CSB MIS Staff whenever significant changes occur. Updates are performed at the direction of the MIS, Director. The MIS Director forwards the updated document to the Executive Director for approval.

Procedures

A. The basic requirements for the Disaster Recover Plan are as follows:
    1. Disaster Recovery Team
    2. Disaster Recovery Documentation
    3. Backup Computer Facilities

B. The Disaster Recover Team (see Attachment A) is established and organized to assess the damage to the computer systems and capabilities, to implement and coordinate recovery/backup actions, and to make recommendations to the Director, MIS. The team consists of persons responsible for one or more of the following functions:
    1. Recovery administration
        a. Insurance Notification
        b. Supplies
        c. Organization
    2. Systems Software
    3. Application Software
    4. Communications
    5. Operations
    6. Facilities
    7. Hardware

    The Director, MIS serves as the Chair. In the absence of the Director, LAN Manager is to serve as the Chair. The Disaster Recovery Team meets quarterly to discuss current documentation and make recommendations for changes. The MIS Director must approve all changes before they are forwarded to the Executive Director for final approval.

    In the event of a disaster or major failure, the team convenes with as many team members as possible. All members of the team assess system and infrastructure damages and report to the Chair at the earliest opportunity.

C. Daily backups of the complete system and databases**,** critical to the restoration of service, are stored in fireproof vaults (see Data Backup and Storage Policy). This policy insures that the most current full system backup and the most recent full database backup are stored far enough away from their respective servers to be safe in the case of fire or flood.

D. In the case of fire or natural disaster it may become necessary to move the computer room to a backup location or alternate site. In the case of localized data center or equipment failure it may not be necessary to move the computer room, however, alternate equipment may be put into service as a temporary measure.

E. Several recovery processes are identified, depending on the circumstances.
    Disaster Preparation.
    Being ready and planning ahead is the easiest way to quickly and fully recover from a disaster. This section outlines the minimum steps needed to insure full recovery from a disaster.

    The LAN manger or designee is responsible for insuring implementation of and compliance with the following requirements:

1. The disaster plan is kept current and all of the personnel on the recovery team are made aware of any changes.
2. The off-site storage area is inspected, at a minimum quarterly, to insure it is clean, organized and that the correct backups are in storage.
3. A full set of the latest version of every file, patch, driver and software package needed to "recreate" the server is created and stored off-site in a locked fire-proof container. The LAN Manager, Facility Manager and MIS Director have the only keys to this storage container and they are each individually responsible for the security of their key.
4. Any fire fighting systems or equipment in the located in network server rooms are properly maintained.
5. Senior staff members are advised of the consequences of a disaster and what they can do while recovery is in progress.
6. The building security and administrative staff have the telephone numbers of persons to contact in the case of an emergency occurring during off hours.
7. Minimum & Recommended specifications for replacement hardware, located in Attachment C, are kept current. The minimum requirements allow for flexibility in acquiring temporary replacement equipment to restore basic services (either full or degraded) during the acquisition of new permanent replacement equipment. .

In the event that there is warning of an impending disaster, e.g. potential flood situations, severe weather activity in the immediate area, fire or potential building damage, the following steps are initiated by the first recovery team member to be made aware of the situation.

1. Notify as many recovery team members as possible. (See Attachment A)
2. The Executive Director and the Director, MIS are briefed and a decision is made whether or not to shut down the systems.
3. The recovery team convenes and develops a remedial plan of action.

Emergency Response.

These are the first actions taken in an emergency situation, designed to bring the computer systems back to operation, even if not at full capacity or in a degraded state.

1. The MIS Director or designee is notified by the first recovery team member made aware of an emergency situation as soon as possible.
2. The MIS Director or designee insures that the Disaster Recovery Team members are notified and assembled as soon as reasonable under the circumstances.
3. Team members assess damages to their individual areas of expertise.
4. Team members advise the MIS Director as to the extent of damage and recovery procedures necessary so that the decision to move the computer center or restart on an alternate equipment platform can be made.
5. All Division Directors are informed, by the designated team member, of the

decision and given an estimated time to the return to either full or degraded service.

6. The Division Directors will notify their staff via the best means available.
7. Disaster Recovery Team members will supervises their own area of expertise.
8. The Information Technology and Purchasing Departments of [Jurisdiction] are contacted, by the designated team member, to determine if needed replacements are available in-house or if emergency purchase orders will need to be created.

Recovery Procedures.

These are the procedures designed to return the computer systems to a fully operational, or a degraded state, including bringing up the alternate site or equipment as circumstances necessitate.

Recovery from a complete failure to a degraded mode of service may be necessary. In this case it may be possible to bring up individual locations on a priority basis. The decision to operate in a degraded mode and the order in which locations are brought back into service is made by the Disaster Recovery Team Leader in consultation with senior staff.
If it is decided to transfer the computer center to the alternate site the following steps will be taken by the designated team member(s):

1. Insure that the basic *Emergency Response* procedures have been followed.
2. Create an inventory of the status of existing equipment (functional or damaged) and files (OK or corrupted).
3. Coordinate the movement of equipment..
4. Contact Information Technology Services and determine equipment availability. If necessary, insure that emergency Purchase Orders are created for replacement equipment.
5. Determine if a new offsite (backup) storage facility is required. If a new site is required, immediately identify the site and coordinate its activation.
6. Test all hardware systems as soon as they are available.
7. Install Network Operating System (NOS), and other low-level software. Create NOS volumes emulating the configuration of the downed server as outlined in Attachment B, Section 2.
8. Communications, networking, operations and applications software personnel prepare to install and or setup their individual function in the appropriate order.
9. Advise Senior Staff of the progress and or impediments on a regular basis.

If it is decided to transfer operations to alternate equipment but not move the data center location, the designated team member(s) will take the following steps:

1. Insure that the basic *Emergency Response* procedures have been followed.

2. Determine the extent of the damage and develop a plan to bring the system back on line.
3. Test all hardware systems as soon as they are available.
4. Install Network Operating System (NOS), and other low-level software. Create NOS volumes emulating the configuration of the downed server as outlined in Attachment B, Section 2. Prepare to support and or adjust individual components
5. Advise Senior Staff of the progress and or impediments on a regular basis.

F. Recovery Timetable--The following timetable does not take into account the amount of time required to input data held on hard copy during the recovery period, or inputting data that may have been lost during recovery. Phases represent units of measure that vary in length depending on the severity of the disaster.

- Phase I — Convene the disaster recovery team and assess damages, determine equipment needs and initiate replacement, discuss options.
- Phase II — Restore programs and data, test integrity of programs and data. Begin restoring communications and networking capabilities.
- Phase III — Restore partial operation to priority locations.
- Phase IV — Determine priority of data processing.
- Phase V — Take delivery and setup new equipment. Restore full communications and networking capabilities. Work with departments to verify data and operation of applications.

G. Disaster Recovery Plan Review -- The following steps are taken to insure that the Disaster Recover Plan is current, feasible and effective:
   1. During January of every year the Disaster Recovery Team convenes to review the Plan and Appendices. Updates or revisions will be made at this time.
   2. The contents of the off-site disaster backup tape storage are subjected to unannounced periodic audits by the LAN Manager or his/her designee. Results of the audit will be documented and reported in writing to the MIS Director.

Attachment A: Disaster Recovery Team

MIS Director

Database Administrator

LAN Manager

Help Desk

Clinical Coordinator

Facilities Manager

Attachment B: Items for Complete System Recovery

Section 1: Software, Data and Documentation

Items needed for complete system recovery of the current servers:

- ☐ ACSB/ACSB2 - HP Netserver LH 6000r/LH 3000
- ☐ RETROSPECT - Dell Optiplex 140
- ☐ ACSBCITIRX - Dell Power Edge 1650

All the below listed items are kept, as per MIS Data Backup and Storage Policy, in a fireproof storage vault.

- ☐ Software to configure the new server's hardware.
- ☐ Bootable install disk to create a Root partition on the server
- ☐ Emergency Recovery Disks for all servers (ACSB, ACSB2, RETROSPECT, ACSBCITRIX)
- ☐ CONFIGURE.txt file of configuration information needed to restore the servers and network connections.
- ☐ Windows NT Advanced Server 4.0.
- ☐ All current Service Packs and Upgrades for NT Server 4.0.
- ☐ Windows 2000 Advanced Server (for ACSBCITRIX)
- ☐ HP Netserver Navigator (M 04.05 or newer)
- ☐ ATM install CD
- ☐ Double-Take CD (v4.2 or newer)
- ☐ NSI activation Code Listing
- ☐ Retrospect software - for backup server
- ☐ Citrix Meta Server XP3 ver. 2.0
- ☐ All required drivers for peripherals and interface cards.
- ☐ Backup tapes.

Section 2: Recovery Procedure

ACSB/ACSB2 procedure:

- ☐ Leave RAID configuration as is.
- ☐ Boot up from HP Netserver Navigator CD to install NT Server Operating System
- ☐ Create an 8 Gigabite Operating System Partion
- ☐ Reinstall NT 4.0 Operating System, Service Pack(s), and Security Updates from Microsoft, in OS partition
- ☐ Recreate Data Partition if necessary.
- ☐ Install Double Take software.
- ☐ Remirror for ACSB2 (or ACSB depending on situation) if possible.
- ☐ Restore for the most recent backup tape if remirroring is not possible.
- ☐ Reconfigure network and ATM settings

- Reconnect to network

RETROSPECT procedure:

- Boot from Install Disk, either NT 4.0 or Windows 2000
- Restore basic partitions
- Install drivers for SCSI card and tape drive
- Install Retrospect Software
- Recreate catalogs from each tape

ACSBCITRIX procedure:

Contact vendor to reinstall and configure Citrix server

Attachment C: System Requirements

Minimum Specifications For MIS Server(s)

The minimum requirements for a temporary ACSB server are:

- DLT backup tape drive
- Processor: 1.2GHz
- Memeory: 1GB
- Storage space: 30GB
- CD ROM
- Network/ATM Interface Card
- Windows NT 4.0 Service Pack 6 (Windows 2000 Server if NT 4.0 is no longer an option)

Recommended Specifications For MIS Server(s)

The recommended server specifications for running the Anasazi system for 250 users and at the current development level of the software are:

- DLT backup tape drive
- Processor : Two Intel Pentium IV 2.0GHz
- Memory: 1GB
- Dual-channel Ultra2 SCSI controller
- Hard drive capacity 120GB
- Network/ATM Interface Card
- Windows 2000 Advanced Server