

Disaster Recovery Plan

Section 1. Major goals of this plan

The major goals of this plan are the following:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

Section 2. Personnel

Data processing personnel

Name	Position	Address	Telephone
-------------	-----------------	----------------	------------------

Note:

Attach a copy of your organization chart to this section of the plan.

Section 3. Application profile

Use the Display Software Resources (DSPSFWRSC) command to complete this table.

Application profile

Application Name	Critical?	Fixed Asset?	Manufacturer	Comments
	Yes/No	Yes/No		

Comment legend:

1. Runs daily_____.
2. Runs weekly on _____.
3. Runs monthly on _____.

Section 4. Inventory profile

Use the Work with Hardware Products (WRKHDWPRD) command to complete this table. This list should include the following:

- Processing units
- Disk units
- Models
- Workstation controllers
- Personal computers
- Spare workstations
- Telephones
- Air conditioner or heater
- System printer
- Tape and diskette units
- Controllers

- I/O processors
- General data communication
- Spare displays
- Racks
- Humidifier or dehumidifier

Inventory profile

Manufacturer Description	Model	Serial Number	Own or Leased	Cost
---------------------------------	--------------	----------------------	----------------------	-------------

Note:

This list should be audited every _____ months.

Miscellaneous inventory

Description	Quantity	Comments
--------------------	-----------------	-----------------

Note:

This list should include the following:

- Tapes
- PC software (such as DOS)
- File cabinet contents or documentation
- Tape vault contents
- Diskettes
- Emulation packages
- Language software (such as COBOL and RPG)

- Printer supplies (such as paper and forms)

Section 5. Information services backup procedures

- iSeries Server
 - Daily, journal receivers are changed at _____ and at _____.
 - Daily, a save of changed objects in the following libraries and directories is done at _____:
 - _____
 - _____
 - _____
 - _____
 - _____
 - _____
 - _____
 - _____

This procedure also saves the journals and journal receivers.

- On _____ (day) at _____ (time) a complete save of the system is done.
- All save media is stored off-site in a vault at _____ (location).
- Personal Computer
 - It is recommended that all personal computers be backed up. Copies of the personal computer files should be uploaded to the server on _____ (date) at _____ (time), just before a complete save of the system is done. It is then saved with the normal system save procedure. This provides for a more secure backup of personal computer-related systems where a local area disaster could wipe out important personal computer systems.

Section 6. Disaster recovery procedures

For any disaster recovery plan, the following three elements should be addressed.

Emergency Response Procedures

To document the appropriate emergency response to a fire, natural disaster, or any other activity in order to protect lives and limit damage.

Backup Operations Procedures

To ensure that essential data processing operational tasks can be conducted after the disruption.

Recovery Actions Procedures

To facilitate the rapid restoration of a data processing system following a disaster.

Disaster action checklist

1. Plan Initiation
 - a. Notify senior management
 - b. Contact and set up disaster recovery team
 - c. Determine degree of disaster
 - d. Implement proper application recovery plan dependent on extent of disaster (see Section 7. Recovery plan--mobile site)
 - e. Monitor progress
 - f. Contact backup site and establish schedules
 - g. Contact all other necessary personnel--both user and data processing
 - h. Contact vendors--both hardware and software
 - i. Notify users of the disruption of service
2. Follow-Up Checklist
 - a. List teams and tasks of each
 - b. Obtain emergency cash and set up transportation to and from backup site, if necessary
 - c. Set up living quarters, if necessary
 - d. Set up eating establishments, as required
 - e. List all personnel and their telephone numbers
 - f. Establish user participation plan
 - g. Set up the delivery and the receipt of mail
 - h. Establish emergency office supplies
 - i. Rent or purchase equipment, as needed
 - j. Determine applications to be run and in what sequence
 - k. Identify number of workstations needed
 - l. Check out any off-line equipment needs for each application
 - m. Check on forms needed for each application
 - n. Check all data being taken to backup site before leaving and leave inventory profile at home location
 - o. Set up primary vendors for assistance with problems incurred during emergency
 - p. Plan for transportation of any additional items needed at backup site
 - q. Take directions (map) to backup site
 - r. Check for additional magnetic tapes, if required
 - s. Take copies of system and operational documentation and procedural manuals.

- t. Ensure that all personnel involved know their tasks
- u. Notify insurance companies

Recovery start-up procedures for use after a disaster

1. Notify _____ Disaster Recovery Services of the need to utilize service and of recovery plan selection.

Note:

Guaranteed delivery time countdown begins at the time _____ is notified of recovery plan selection.

- a. Disaster notification numbers
_____ or _____

These telephone numbers are in service from _____ am until _____ pm Monday through Friday.

2. Disaster notification number: _____

This telephone number is in service for disaster notification after business hours, on weekends, and during holidays. Please use this number only for the notification of the actual disaster.

3. Provide _____ with an equipment delivery site address (when applicable), a contact, and an alternate contact for coordinating service and telephone numbers at which contacts can be reached 24 hours a day.
4. Contact power and telephone service suppliers and schedule any necessary service connections.
5. Notify _____ immediately if any related plans should change.

Section 7. Recovery plan-mobile site

1. Notify _____ of the nature of the disaster and the need to select the mobile site plan.
2. Confirm in writing the substance of the telephone notification to _____ within 48 hours of the telephone notification.
3. Confirm all needed backup media are available to load the backup machine.
4. Prepare a purchase order to cover the use of backup equipment.
5. Notify _____ of plans for a trailer and its placement (on _____ side of _____). (See the Mobile site setup plan in this section.)

6. Depending on communication needs, notify telephone company (_____) of possible emergency line changes.
7. Begin setting up power and communications at _____.
 - a. Power and communications are prearranged to hook into when trailer arrives.
 - b. At the point where telephone lines come into the building (_____), break the current linkage to the administration controllers (_____). These lines are rerouted to lines going to the mobile site. They are linked to modems at the mobile site.

The lines currently going from _____ to _____ would then be linked to the mobile unit via modems.

- c. This could conceivably require _____ to redirect lines at _____ complex to a more secure area in case of disaster.
8. When the trailer arrives, plug into power and do necessary checks.
9. Plug into the communications lines and do necessary checks.
10. Begin loading system from backups (see Section 9. Restoring the Entire System).
11. Begin normal operations as soon as possible:
 - a. Daily jobs
 - b. Daily saves
 - c. Weekly saves
12. Plan a schedule to back up the system in order to restore on a home-base computer when a site is available. (Use regular system backup procedures).
13. Secure mobile site and distribute keys as required.
14. Keep a maintenance log on mobile equipment.

Mobile site setup plan

Attach the mobile site setup plan here.

Communication disaster plan

Attach the communication disaster plan, including the wiring diagrams.

Electrical service

Attach the electrical service diagram here.

Section 8. Recovery plan-hot site

The disaster recovery service provides an alternate hot site. The site has a backup system for temporary use while the home site is being reestablished.

1. Notify _____ of the nature of the disaster and of its desire for a hot site.
2. Request air shipment of modems to _____ for communications. (See _____ for communications for the hot site.)
3. Confirm in writing the telephone notification to _____ within 48 hours of the telephone notification.
4. Begin making necessary travel arrangements to the site for the operations team.
5. Confirm that all needed tapes are available and packed for shipment to restore on the backup system.
6. Prepare a purchase order to cover the use of the backup system.
7. Review the checklist for all necessary materials before departing to the hot site.
8. Make sure that the disaster recovery team at the disaster site has the necessary information to begin restoring the site. (See Section 12. Disaster site rebuilding).
9. Provide for travel expenses (cash advance).
10. After arriving at the hot site, contact home base to establish communications procedures.
11. Review materials brought to the hot site for completeness.
12. Begin loading the system from the save tapes.
13. Begin normal operations as soon as possible:
 - a. Daily jobs
 - b. Daily saves
 - c. Weekly saves
14. Plan the schedule to back up the hot-site system in order to restore on the home-base computer.

Hot-site system configuration

Attach the hot-site system configuration here.

Section 9. Restoring the entire system

To get your system back to the way it was before the disaster, use the procedures on recovering after a complete system loss in the *Backup and Recovery*, SC41-5304-06.

Before You Begin: Find the following tapes, equipment, and information from the on-site tape vault or the off-site storage location:

- If you install from the alternate installation device, you need both your tape media and the CD-ROM media containing the Licensed Internal Code.
- All tapes from the most recent complete save operation
- The most recent tapes from saving security data (SAVSECDTA or SAVSYS)
- The most recent tapes from saving your configuration, if necessary
- All tapes containing journals and journal receivers saved since the most recent daily save operation
- All tapes from the most recent daily save operation
- PTF list (stored with the most recent complete save tapes, weekly save tapes, or both)
- Tape list from most recent complete save operation
- Tape list from most recent weekly save operation
- Tape list from daily saves
- History log from the most recent complete save operation
- History log from the most recent weekly save operation
- History log from the daily save operations
- The *Software Installation* book
- The *Backup and Recovery* book
- Telephone directory
- Modem manual
- Tool kit

Section 10. Rebuilding process

The management team must assess the damage and begin the reconstruction of a new data center.

If the original site must be restored or replaced, the following are some of the factors to consider:

- What is the projected availability of all needed computer equipment?
- Will it be more effective and efficient to upgrade the computer systems with newer equipment?
- What is the estimated time needed for repairs or construction of the data site?
- Is there an alternative site that more readily could be upgraded for computer purposes?

Once the decision to rebuild the data center has been made, go to Section 12. Disaster site rebuilding.

Section 11. Testing the disaster recovery plan

In successful contingency planning, it is important to test and evaluate the plan regularly. Data processing operations are volatile in nature, resulting in frequent changes to equipment, programs, and documentation. These actions make it critical to consider the plan as a changing document. Use these checklists as you conduct your test and decide what areas should be tested.

Table 3. Conducting a recovery test

Item	Not			Comments
	Yes	No	Applicable	
Select the purpose of the test. What aspects of the plan are being evaluated?				
Describe the objectives of the test. How will you measure successful achievement of the objectives?				
Meet with management and explain the test and objectives. Gain their agreement and support.				
Have management announce the test and the expected completion time.				
Collect test results at the end of the test period.				
Evaluate results. Was recovery successful? Why or why not?				
Determine the implications of the test results. Does successful recovery in a simple case imply successful recovery for all critical jobs in the tolerable outage period?				
Make recommendations for changes. Call for responses by a given date.				
Notify other areas of results. Include users and auditors.				
Change the disaster recovery plan manual as necessary.				

Table 4. Areas to be tested

Item	Not			Comments
	Yes	No	Applicable	
Recovery of individual application systems by using files and documentation stored off-site.				
Reloading of system tapes and performing an IPL by using files and documentation stored off-site.				
Ability to process on a different computer.				
Ability of management to determine priority of systems with limited processing.				
Ability to recover and process successfully without key people.				
Ability of the plan to clarify areas of responsibility and the chain of command.				
Effectiveness of security measures and security bypass procedures during the recovery period.				
Ability to accomplish emergency evacuation and basic first-aid responses.				
Ability of users of real-time systems to cope with a temporary loss of on-line information.				
Ability of users to continue day-to-day operations without applications or jobs that are considered noncritical.				
Ability to contact the key people or their designated alternates quickly.				
Ability of data entry personnel to provide the input to critical systems by				

using alternate sites and different input media.

Availability of peripheral equipment and processing, such as printers and scanners.

Availability of support equipment, such as air conditioners and dehumidifiers.

Availability of support: supplies, transportation, communication.

Distribution of output produced at the recovery site.

Availability of important forms and paper stock.

Ability to adapt plan to lesser disasters.

Section 12. Disaster site rebuilding

- Floor plan of data center.
- Determine current hardware needs and possible alternatives. (See Section 4. Inventory profile.)
- Data center square footage, power requirements and security requirements.
 - Square footage _____
 - Power requirements _____
 - Security requirements: locked area, preferably with combination lock on one door.
 - Floor-to-ceiling studding
 - Detectors for high temperature, water, smoke, fire and motion
 - Raised floor

Vendors

Floor plan

Include a copy of the proposed floor plan here.

Section 13. Record of plan changes

Keep your plan current. Keep records of changes to your configuration, your applications, and your backup schedules and procedures. For example, you can get print a list of your current local hardware, by typing: