DISASTER RECOVERY PLAN

Section 1. Goals of a Disaster Recovery Plan

The major goals of a disaster recovery plan are:

- To minimize interruptions to 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 network engineers and managers on emergency procedures.
- To provide for smooth and rapid restoration of service.
- Establishing high WAN/Internet connection reliability and fault tolerance.
- The following is a list of all IT personnel who are involved with information technology aspects. This list should be updated frequently.

Section 2. Personnel

Data Processing Personnel			
Name	**Position**	**Address**	**Telephone**

Section 3. Application Profile

This is a list of all application personnel who are involved with payroll, accounts payable/receivable, orders, etc.

Application Profile				
Application Name	**Critical? Yes or No**	**Fixed Asset? Yes or No**	**Manufacturer**	**Comments**

Comment Legend:

1. Runs Daily
2. Runs Weekly On
3. Runs Monthly On

Section 4. Inventory Profile

This is a list of physical inventory that involves your LAN & WAN. This list should be updated frequently and should include all components to your network. 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
- Power Generator?

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
- File cabinet contents or documentation
- Tape vault contents
- Diskettes
- Emulation Packages
- Language Software
- Printer Supplies

Section 5. Information Services Backup Procedures

This procedure saves the journals and journal receivers.

- On _____ (day) at _____ (time) a complete save of the system is done.

- All saved 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.

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 _____).

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.
11. Begin normal operations as soon as possible:
    a. Daily Jobs
    b. Daily Saves
    c. Weekly Saves
12. Plan a schedule to backup 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 writing 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.
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.
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 saved tapes.
13. Begin normal operations as soon as possible.
14. Plan the schedule to backup the hot-site system in order to restore on the home-base computer.

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 sections.

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 your configuration, if necessary
* All tapes from the most recent daily save operation
* Tape list from most recent complete, weekly, and daily save operations
* History log from the most recent complete, weekly, and 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?

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 this checklist as you conduct your test and decide what areas should be tested:

Conducting a Recovery Test:

Item	Yes	No	Applicable	Not Applicable	Comments
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.					
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 tests 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.				

Areas to be Tested:

Item	Yes	No	Applicable	Not Applicable	Comments
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 not critical.					
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, and communication.					
Distribution of output produced at the recovery site.					
Availability of important forms and paper stock.					
Ability to adapt plan to lessen 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

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.

Vendors – Include Vendor Information Here			
Company Name	**Contact**	**Address**	**Telephone**