[Company Name]

Contingency Plan

Introduction

This contingency management plan describes the methods and procedures to be used by [Company Name] in order to safeguard and restore data center operations, in the event of a disaster.

The body of this [Company Name] contingency plan is presented in four sections:

I Disaster Recovery Plan

A. *Disaster Recovery Services* - a summary of the recommended services necessary to implement this plan

B. *Disaster Recovery Planning and Documentation* - review of internal disaster recovery plans and procedures.

C. *Disaster Recovery Checklist* - a high-level "play-script" that outlines the sequence of steps to be followed in implementing temporary operations and in restoring full normal operations after a disaster occurs.

D. Disaster Recovery Plan Testing Procedure

II Data Backup Plan

E. *Data Backup Services* – a summary of the recommended services necessary to implement this plan.

F. Data Backup Procedure

G. Data Restore Procedure

H. Data Backup and Restore Testing Procedure

III Emergency Mode Operation Plan

A. *Emergency Mode Operation Services* - a summary of the recommended services necessary to implement this plan.

B. Emergency Mode Operation Procedure

C. Emergency Mode Operation Testing Procedure

IV Appendix

A. Applications and Data Criticality Analysis

B. Information Systems Survey

C. Evaluation of Testing and Revision (if applicable)

D. Contact numbers of Disaster Recovery Team

E. Vendor/contractor contact list

I. Disaster Recovery Plan

A. Disaster Recovery Services

[Company Name] currently operates (data centers, networks, other systems). The (data centers, networks, other systems) support (operations, # users, locations).

(Other operating parameters of data centers, networks, other systems)

(Current Disaster Recovery capabilities)

(Vendor capabilities, if Disaster Recovery was outsourced)

(Summary of Disaster Recovery Plan – time to recover, on-site or off-site locations, vendors, budget/cost, people)

B. Disaster Recovery Planning and Documentation

The narrative outline below defines the basic organizational and planning elements that need to be addressed.

1. Disaster Definition and Reaction

A.	For purposes of this discussion, a disaster is considered any incident or event that results in a major (multi-day) interruption of operations at one or more of the [Company Name] data centers. For disruptions in service that affect only a portion of systems or operations at any one location, a subset of the full recovery procedures will likely be used to restore normal operations. A catastrophic disaster, however, would render the [Company Name] incapable of conducting critical functions for an extended period of time. The impact of such a disruption would require that notification and periodic updates be circulated throughout the System, until normal operations were restored. The appropriate authorities, depending on the nature of the disaster (fire, flood, etc.), would also have to be contacted. Personnel at each [Company Name] location, organized into emergency management teams, would coordinate the initial response to the disaster, assess the damage, and determine the extent to which all or part of the disaster recovery plan should be deployed. Designated team members would have responsibility for maintaining the necessary sequence of notifications to senior management, to users, to public emergency personnel, and to [Company Name] contractors, as appropriate and as the need arises. To insure preparedness for emergency responses, each designated staff, as well as senior managers, should maintain a copy of this contact list, as well as a copy of the full disaster recovery plan, at their residences.

2. Preparation for Recovery

Emergency management responses will be premised on the existence of certain back-up measures essential to temporary restoration of services, which are listed in the Data Backup Plan.

- Assurance of emergency equipment
- Availability of the alternate [Company Name] site and connectivity.
- Documentation of hardware and software to be replaced and/or restored
- Preservation of system and data back-up tapes

The above four elements are the basic ingredients necessary to restore operations after destruction or loss of any major component or an entire site. (It must be assumed that personnel with the necessary skills and abilities are available and can communicate with and/or relocate to the alternate site at which temporary operations are to be established.)

Additional preparatory actions include:

- Contact equipment replacement provider to initiate declaration of disaster and delivery of hardware
- Notify hardware maintenance providers of disaster condition and disposition of affected equipment
- Notify software providers of disaster condition and imminent need for new software keys, as appropriate, upon identification of serial numbers of replacement equipment
- Retrieve most recent back-up tapes and transport them to alternate location

To aid in accomplishing these steps, **Appendix E** provides a vendor/contractor list that lists hardware, software and off-site storage contractor information.

3. Implementation of Temporary Operations

Upon establishment of a "control center" (e.g., the computer facilities at the alternate back-up site and/or the nearest available offices or temporary work area), emergency management team members would initiate the steps necessary to reinstate operations from the new location. Ideally, the team would keep a disaster recovery log to aid in the preparation of status reports and to document the incident for historical purposes. Working from procedural and recovery checklists (copies of which should be maintained with the back-up tapes and with key copies of the disaster recovery plan), they would proceed to:

1. Assemble and verify availability of all necessary hardware, software, and resources at the back-up site
2. Install and test systems and applications software
3. Arrange for and test/verify full recovery of communications capabilities
4. Determine starting point for recovered operations
    A. establish latest back-up files to be restored
    B. establish priority sequence for restoring most critical applications

C. revise production schedules
D. alert the user community to status and potential gaps in data and/or changes in procedures (i.e., need to re-enter lost data or resubmit requests/reports, etc.)

5. Monitor and verify restoration is complete and data integrity and continuity have been re-established
6. Resume full processing schedule

Of course, these steps can only be realized if all basic/normal testing and production procedures have been well documented and an Applications and Data Criticality Analysis has been completed and documented.

4. Restoration of Normal Operations

Once the back-up facility is functioning on a full production schedule, attention would return to the permanent data center. Initial assessments of damage would be refined, and reconstruction plans developed. If major facilities/site damage had been incurred, the full reconstruction plans would extend well beyond [Company Name] Data Center operations and staff. However, once the time schedule for facilities reconstruction were known, at least approximately, plans could be made for permanent replacement equipment. Unless arrangements had been made to continue long-term lease (or purchase) of the temporary replacement equipment, this undertaking would entail issuance of a competitive solicitation for the replacement hardware. Award/delivery would have to be timed to coincide with availability of a reconstructed data center. With the permanent center restored, operations are transferred from the temporary facility by following the same sequence of steps as were used to set up the back-up site. The re-establishment of normal operations should proceed under far less duress than the establishment of emergency operations, and the logs kept during disaster recovery should help highlight and troubleshoot/resolve any problems that may have arisen during earlier system transfers.

a) Access to Facilities

In order to initiate the recovery procedure, information systems staff will need access to facilities and information systems to support the recovery process. Disaster recovery team members will be given clearance and access to facilities during the recovery phase.

C. Disaster Recovery Procedure

1. Phase 1

- Notify disaster planning/disaster recovery coordinator
- Upon occurrence of any disaster that causes interruption of service at either [Company Name] data center, contact [Security Officer]. He is currently acting as primary disaster recovery coordinator. In the event he is unavailable, [Names] shall act as secondary, back-up contacts/coordinators.
- Assess nature and impact of emergency
- Within the first 2 hours after notification, the disaster recovery coordinator will:
  - assess damage
  - notify senior management

  - make decisions on immediate course of actions (determine if recovery is feasible in place, at the affected location, or if the alternate site must be mobilized as the back-up)
  - notify engineering and operations response team leaders
  - give formal notification to [Hot Site Provider], to declare a disaster and initiate replacement equipment shipment (to the affected site, if possible, or the alternate site, as circumstances dictate)
- Follow through on notifications

2. Phase 2

- Within 4 hours, the disaster recovery coordinator will:
  - contact the Customer Support Services manager with the information necessary to provide an initial status report to customer service liaisons and users, in general
  - contact off-site storage provider (as needed)
  - confer with operations team(s) to schedule duties for obtaining/recovering backup tapes and associated data/documentation
  - confer with engineering team(s) to coordinate site readiness for connection of replacement equipment and rerouting of telecommunications links, as needed
  - Complete recovery preparations
- Within 8 hours, the disaster recovery coordinator will:
  - provide senior management with an updated assessment, including estimated recovery schedule
  - arrange for emergency funding, if required to cover travel or any other extra expenses necessary to deal with the situation
  - contact software providers to alert them to anticipated interim operations requirements, need for emergency software keys, etc.
- The operations team(s) will be proceeding with retrieval/recovery of back-up tapes.
- The engineering team(s) will be coordinating restoration at the affected or alternate site, as appropriate.
- Both teams will initiate their portions of recovery logs.
- Establish a basis for interim operations

3. Phase 3

- Within 36 hours, if replacement equipment is not yet available, the disaster recovery coordinator, in concert with operations and engineering team captains will:
  - initiate an alternate production schedule to share the resources of the remaining site to support operational requirements for site(s)
  - test and verify communications capabilities
- Within 48 hours:
  - the disaster recovery coordinator will provide updates to senior management
  - notification of alternate/interim processing schedules will be issued
  - Re-establish a full processing schedule
- Upon delivery of replacement equipment (within 5 days after the disaster occurs), operations and engineering teams will:
  - install and test all applications software on replacement hardware
  - restore data on replacement equipment
  - monitor restored operations to verify continuity, data integrity, etc.
  - resume full processing schedules

4. Phase 4

- Within 5 to 7 days, the disaster recovery coordinator will:
  - provide updates to senior management
  - announce the resumption of full processing schedules
  - conclude the disaster recovery logs documenting restoration of operations
- Restore normal operations

If the above steps resulted in restoration of operations at the affected site:

- re-assess status of equipment (necessity of bidding permanent replacement equipment, while continuing [Hot Site Provider] lease, etc.)
- re-assess any other physical/facilities requirements before considering restoration complete
- confirm status of hardware/software with vendors/service-providers

If the above steps resulted in restoration of operations at the alternate site:

- work with facilities and other groups to restore original site
- work with procurement and other groups to purchase permanent replacement equipment
- install permanent replacement hardware
- transport back-up tapes to restored site
- re-install all operating systems, applications software, data, etc.
- test and verify all systems are operational
- re-route and test communications to restored site
- announce restoration and re-scheduling of operations from restored site
- resume all restored/normal operations

D. Disaster Recovery Plan Testing Procedure

____

____

____

____

II. Data Backup Plan

A. Data Backup Services

Critical data and applications will be backed up using (in-house, offsite) resources on a regular (daily, weekly, monthly) basis.

Critical data were identified as:

____

Critical applications were identified as:

____

(Current backup capabilities)

____

(Vendor capabilities, if backup was outsourced)

____

B. Data Backup Procedure

____

____

____

____

C. Data Restore Procedure

____

____

____

____

D. Data Backup and Restore Testing Procedure

III.Emergency Mode Operation Plan

For purposes of this discussion, an emergency is considered any incident or event that results in a temporary interruption of operations at one or more of the [Company Name] data centers, or in disruptions in service that affect only a portion of systems or operations at any one location. A catastrophic disaster, however, would render the [Company Name] incapable of conducting critical functions for an extended period of time. The impact of such a disruption would require that notification and periodic updates be circulated throughout the System, until normal operations were restored. The appropriate authorities, depending on the nature of the disaster (fire, flood, etc.), would also have to be contacted. Personnel at each [Company Name] location, organized into emergency management teams, would coordinate the initial response to the disaster, assess the damage, and determine the extent to which all or part of the disaster recovery plan should be deployed. Designated team members would have responsibility for maintaining the necessary sequence of notifications to senior management, to users, to public emergency personnel, and to [Company Name] contractors, as appropriate and as the need arises. To insure preparedness for emergency responses, each designated staff, as well as senior managers, should maintain a copy of this contact list, as well as a copy of the full disaster recovery plan, at their residences.

A. Emergency Mode Operation Services

Emergency mode operation will be initiated using (in-house, offsite) resources on an emergency basis.

Critical data were identified as:

Critical applications were identified as:

(Current emergency mode capabilities)

(Vendor capabilities, if emergency mode operation was outsourced)

B. Emergency Mode Operation Procedure

C. Emergency Mode Operation Testing Procedure