SMB

Disaster Recovery Plan

Generic Company Name

Information Services Department

1.0 Introduction

The Information Services Department provides services that, in some manner, virtually every other department at XXX is dependent upon. Without telephones, or networks, or any one of several critical servers, or some other computing resource, many aspects of the business would come to a standstill if a failure occurred. In recognition of these dependencies, it is of utmost importance that the IS Department be prepared to respond to a disaster in an orderly, timely and efficient fashion.

This document describes the Disaster Recovery Plan that the IS department will use in the event that a catastrophic event affects department operations by impacting IT systems and services. It includes a summary of the current services, identification of the services most critical to company operations, and how these services will be reconstituted following a disaster.

1.1 Scope of This Plan

This plan provides the IS department with the ability to address two areas:

1. It enables the department to restore YourCompany's core information systems in the event of a disaster.
2. It identifies areas of substantial risk and exposure to disaster, and helps us reduce these risks.

This plan is not intended to be a detailed, step by step series of instructions to follow. Rather, it is intended to be a roadmap to lead the recovery team from the incident, through a decision making process, to implementation of restored services. Although it is targeted at the most likely types of disasters that could be encountered, it may be adapted as necessary for recovery from other situations.

1.2 Disaster Scenarios

This plan focuses on recovering from an event that causes partial destruction of one or more, but not all, buildings at YourCompany's corporate headquarters in SomeCity, STATE.

The building deemed most critical is THEDATACENTERBUILDING, where IS houses it's core systems. Secondary facilities for network services are located at XXX and XXX streetaddress.

2.0 Current Practices & Procedures

An understanding of the fundamental business practices currently followed by the department is essential to recovering department operations. The key activities include:

- Data backup & restoration
- Server & systems administration
- System shutdown and startup
- Identification of critical systems

2.1 Data Backup & Restoration

Full backups are performed each weekend with incremental backups occurring each weeknight. Restoring a server therefore requires recall of the previous full backup and incrementals for each subsequent day.

Backup tapes for each week are collected and stored in the Server Room. Each day the collection is shipped to OFFSITE STORAGE COMPANY'S branch for offsite storage. Long term archives are set aside monthly (retained for one year) and annually (retained for three years).

Key servers across all UNIX, NT, and Mac platforms are included in the backup schedule.

2.2 Server & System Administration

Current practice for managing servers and desktop systems across the company include:

- Ensuring high availability of servers during business hours
- User support and desktop system support during normal business hours
- Weekly scheduled outages for critical servers
- Other major server maintenance is scheduled outside of normal business hours

2.3 System Shutdown & Startup

Instructions for shutdown and startup of critical servers will be located in the Server Room and attached to this plan as Appendix A. These procedures cover the servers in the Server Room as well as network components across the campus.

2.4 Critical Systems

The systems, services and functions identified as necessary to current business operations are as follows. Some systems listed are located outside of YourCity, but are listed here due to their dependency on YourCity based services. Without awareness of these remote systems, it is possible that an oversight during a restoration could result in a continued outage at a remote site.

Category	Hostname or Description	Functionality Provided
UNIX Systems		
Voice Communications		
Network Services		
Applications Servers		
DBMCs		
NT Systems		
MAC Systems		
Windows Workstations		
AS/400 Systems		

Category	Hostname or Description	Functionality Provided
z/OS Servers		

3.0 Recovery Operations

Re-establishing operations after a disaster requires:

- A process to follow as a guide for recovery
- Identification of the most critical services provided by the department
- Priorities for re-establishing those services
- The staff required for a recovery
- System configuration information

3.1 Recovery Process

The recovery process consists of two basic phases:

1. An initial reaction phase where notifications are made, the staff assembled, information gathered, and an action plan developed.
2. The recovery phase, where resources are acquired, data recalled, and services are restored as much as possible.

The steps to be followed are:

1. The discoverer of a disaster will notify the people below. Each of these people will notify others, as appropriate. For situations during normal business hours, personal contact will be made; for a disaster outside of normal business, the nationwide paging service (XXX-XXX-XXXX) will be used to place an urgent page.
    - Facilities manager
    - IS director
    - Any company executive
    - Local authorities (911) in the event outside assistance is necessary.

2. Initial organization and preparation for the recovery:
    - Notify & assemble the recovery staff (Listed in Section 3.4)
    - Review this recovery plan with the staff
    - Organize for damage assessment
    - Establish communications systems for the staff
    - Assign duties and responsibilities to the staff

3. Perform a damage assessment:
    - Conduct a site survey of the affected area
    - Inventory any salvageable or usable equipment

4. Plan for recovery:
    - Compile a master inventory of salvageable equipment
    - Review the overall damage with the recovery staff
    - Develop a detailed action plan
    - Notify the appropriate vendors and service providers
    - Communicate status to executive staff

5. Salvage operations:
    - Recover all salvageable hardware
    - Service or refurbish equipment as necessary

6. Re-establish services in their order of priority as listed in Section 3.2:
    - Priority 1 services
    - Priority 2 services
    - Priority 3 services
    - ISP based services

3.2 Critical Services & Recovery Priorities

Recovery operations are prioritized based on company needs. These priorities are:

Priority	Action	Details
1	Secure and set up a location	Equipment Room
		Equipment racks, tables, shelves
		Cable Plant
		Power
		Cooling
1	Establish Telephone Service	PBX
		Voicemail
		Phone Service to Recovery Site/Staff
		Phone Service to Executive location/Staff
1	Establish LAN Services	Hubs, routers, switches
		Cabling
1	Install Servers	NIS Services
		Primary Domain Controller
		File Servers
		Mail Servers
		Directory Servers
		Home Directory Server
		Backup/Restore Server
1	Stanly connectivity to the wide area network	Hubs, Routers. Etc.
		IP Changes
		Service provider
		Other equipment installation
2	Re-establish Business Systems	Payroll
		Application 1
		Application 2
3	Establish all remaining Services	

3.3 Equipment List

Please refer to Appendix B for a listing of the equipment that is required to re-establish IT services to the clients. Appendix B recommends which equipment is required in order to restore Priority 1, 2 and 3 services listed above to a basic, nominal level of service. It is not intended to duplicate the original performance, but rather to provide a minimally acceptable level of service.

This equipment may be provided by a hotsite vendor, obtained from YourCompany's normal vendors, or it may be deployed from the salvaged equipment pool.

3.4 Recovery Team

The initial response team will consist of all on-call staff, managers, and the director. The remaining department staff will be called in as required to work later shifts. Should additional staff be required at initial response, managers will contact the appropriate people.

3.5 System Configuration Information

The hardware listed above will require configuration to restore reasonable levels of service. The information, data, applications, and instructions required for this are:

- Root and administrative passwords for servers, applications, and network hardware. This information is currently located in the lockbox in the Server Room.
- Configuration information for existing critical systems. This knowledge is currently shared across the department staff, with some documentation in place. This information will be collected in a department directory on YourMachine:/home/is. Future documentation will be placed here as it is developed. This directory will be included in the backup schedule to ensure the information is present for recovery purposes.
- Media containing operating systems, applications, and installed software and licenses.

THE OFFSITE STORAGE COMPANY will provide a document container for storage of configuration information. This container will include a copy of:

- An envelop from each IS group containing current administrative and root passwords. The envelop will be sealed and marked with a description of it's

content and the date.

- OS packs for Solaris xxx and SunOS xxx
- CD-ROMs for Oracle and Clarify applications.
- Application CD-ROMs for backup and restore programs for all platforms.
- YourCompany's custom CD-ROM for Tier 1 & 2 Mac & PC software.
- Network hardware CD-ROMs.
- A copy of this plan.

As information changes and media is updated, copies will be forwarded to the department's Arcus liaison for submission to the container. The container will be recalled from THE OFFSITE STORAGE COMPANY and it's contents updated.

All other applications will be obtained from normal vendors.

4.0 Plan Administration

This plan is subject to review by IS department personnel at six month intervals. Revisions will consider service improvements and advancements as well as changing business needs.

4.1 Document Distribution

This document is company property that is distributed to all IS department personnel. It will be kept off site by each staff member in a secure location. Possession of this document will be noted in each person's personnel file, and the document is to be surrendered upon termination of employment or transfer outside of the IS department.

Additional copies of this plan will reside in the Server Room, the document container at THE OFFSITE STORAGE COMPANY, and in electronic form in the UNIX IS common file storage subdirectory.

4.2 Revision History

Description	Date
Initial Release	

Appendix A: System Shutdown & Startup Procedures

System shutdown and startup procedures for all critical systems including all server and the telecommunications system have been developed as an independent project. They are included here as reference attachments for each identified critical system.

Appendix B: Hardware Inventory

An important component to any recovery plan is an equipment inventory. At a minimum this should include:

- a listing of all equipment by type and model number
- associated software packages, with version number
- date of purchase; and
- original cost
- A description of the applications or services that the equipment supports

Appendix C: Software Inventory

This inventory should include:

- the purpose of the software
- the acquisition date of the software
- the original cost of the software
- the license number; and
- the version number
- current maintenance level

Appendix D: Network Diagram

Appendix E: Personnel Notification Procedure & Contact List

Appendix F: Vendor Contact List