Your Company Name

Disaster Recovery Plan Information

Date

Revision History

Date	Version	Author	Change

Table of Contents

Note: Text displayed in blue italics is included to provide guidance to the author and should be deleted before publishing the document. In any table, select and delete any blue line text; then click Home→Styles and select "Table Text" to restore the cells to the default value.

1 Purpose

Purpose describes the intent of the document, which is to provide disaster recovery (DR) plan information in the event of a crisis or an emergency situation that warrants movement to another location.

1.1 What is Disaster Recovery

Disaster recovery is the process whereby a company would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

A disaster recovery plan is part of an overall contingency plan to complete that restoration task and keep the company running. A disaster recovery plan is required for any publicly traded company and companies that need to minimize loss. This disaster recovery declaration plan is designed for conditions under which the company site is unable to function under standard daily business procedures.

1.2 Goals, Objectives, and Scope

This section describes the goals, objectives, and scope of the plan, e.g.,

- ***Intent of the plan***
- ***What it will address***
- ***What scenarios are being planned for***
- ***Timeframes considered, and***
- ***Other planning assumptions.***

2 General Disaster Plan Information

2.1 Disaster Recovery Team

The disaster recovery team is composed of a predefined group of employees from various business units of the company. These employees should be trained to perform their disaster recovery responsibilities.

Provide Disaster Team Member information in the following table.

Team Member	Area of Responsibility	Work Telephone #	Home Telephone #	Cell #
	Information Technology			
	Human Resources			
	Accounting			
	Tax			
	Treasury			
	Operations			
	Legal			
	Communication			
	Disaster Recovery Site Provider			

2.2 Disaster Recovery Time

Recovery time to start and maintain operations is vital to the financial needs of the company. The following are sample categories and tiers to begin operations, services, and technology in the event of a disaster: The organization needs to define those items.

Disaster Recovery Category	Recovery Time
Infrastructure	*0-8 Hours*
Mission Critical or Tier One	*8-24 Hours*
Mission Essential or Tier Two	*24 - 48 Hours*
Business Unit Essential or Tier Three	*48 - 72 Hours*
Business Unit Essential or Tier Four	*120+ Hours*
New applications not yet assigned a criticality ranking.	*To be determined; defaults to priority 4 until management approval is received of a different priority*

2.3 Disaster Recovery Site

A disaster recovery site should be pre-configured specifically for disaster circumstances. The location of the disaster recovery site is: (Enter location here).

2.4 Critical Services or Information

Provide a methodology to ensure that mission critical services are identified. See the following table with example information.

Service or Information	Description
Revenue Dependent Technology Services	*Services where the company's revenue would be directly impacted if certain technology services are not available are given the highest priority. Data required for these services will be copied to the disaster recovery site in real time in the event of an emergency.*
Productivity Services	*These technology services allow the company to work more productively and save operating expenses. These services will be prioritized from an economical standpoint.*
Technology Infrastructure	*These are the basic technology services required by business operations such as redundant electrical, cooling, network, security, internet access, telephones, email, etc.*
Employee Offices	*Offices space for "X" number of employees at the disaster recovery site. The site will be configured for easy remote access from home*

Service or Information	Description
	locations for employees who will not have access to office space.
Technology Equipment	*To minimize costs in the event of a disaster, employees could bring their laptops. Other equipment should be purchased quickly to meet computing needs if necessary.*

2.5 Technology Priority for Services and Applications

Categorize technology services and applications according to the priority in which they will be recovered under disaster conditions. This priority categorization is part of a joint effort between the Information Technology staff and the Business Unit employees who use the specific technology services or applications. The priority settings should be approved by senior management and not be changed without proper approval.

Provide information on how services, applications, and databases will be restored (e.g., timeframe, recovery tier, point of failure, last offsite backup, intraday backup, etc.). The following table shows recovery category examples.

2.5.1 Disaster Recovery Areas-Examples

Office Space & Technology Infrastructure – Revenue Dependent Technologies

These technology services are essential to the company's revenue stream.

- Recovery Time: 0 – 8 Hours
- Equipment Strategy: Equipment on site for immediate technology requirements

Service	Description
Company Network	
Email	
Internet	
Telecommunications & Voice Mail	
Windows Server- Security and shared network drives.	

Tier One & Two – Operational Productivity Technologies

The technology services in tiers one and two allow the company to operate efficiently using automated processes in daily business operations.

- Recovery Time: 24 – 48 Hours
- Equipment Strategy: Equipment on site to meet aggressive recovery commitments.

Service	Description
Communications	
Finance	
Human Resources	
Information Technology-to corporate applications	

Tier Three – Operational Productivity Technologies

Tier three applications provide productivity improvements and are not revenue dependent.

- Recovery Time: 48 – 72 Hours
- Equipment Strategy: Equipment contract in place for guaranteed 24 hour delivery.

Service	Description
Operations and Maintenance	

Tier Four – Operational Productivity Technologies – 120+ Hour Recovery

The technology services in tier four are the lowest priority items that are not time sensitive. They will be recovered in relation to their respective priorities depending on the timing of any disaster condition.

Service	Description
Finance, e.g., • ***Accounting GL Reporting*** • ***Expense Account Reporting*** • ***Property Tax Management***	
Information Technology, e.g., • ***Computer Management*** • ***IT Help Desk***	
Legal	

3 Response Process

3.1 Notice of Problem

Provide information about how to report a problem to management or staff, e.g., by phone or email.

3.2 Problem Assessment

Provide information on how to perform the initial analysis.

3.3 Problem Resolution

Provide information about how to resolve a problem, e.g., the following table provides a sample methodology to resolve problems.

Incident Information	Resolution
Category 1, routine incident	*Use normal help desk or on-call procedures.*
Category 2 or 3 incident	*Help Desk (during the day) or on-call person (after hours) notifies team management. Start the assessment process and escalate the incident if necessary.*
Category 4 incident	*Notify the head of IT and the Local IT Disaster Recovery coordinator and implement Disaster Recovery procedures.*
Notify the Incident Manager of the incident	*Incident Manager starts the damage specific shift assignments with communication to appropriate employees.* • *Activate the Disaster Recovery Plan.* • *Start damage assessment process.* • *Prepare damage report and incident severity.* • *Determine Incident Command Team assignments, e.g., determine timeframe to setup other teams, contact Team Leaders, and request non-critical staff to remain at home until further notice.* *Make decision (yes/no) to relocate data center processing to backup site.* • *Designate Recovery Team(s), leaders, and staff.* • *Notify team(s) of disaster.* • *Implement the recovery plan.*

3.4 Disaster Condition Declaration

Define how and when a disaster declaration can be declared, e.g.,

Authorization: A minimum of two (2) members of the company's senior management team should have the authority to declare a disaster recovery condition. When a disaster recovery condition is declared by senior staff the following initial steps should be initiated:

Notify the following individuals or groups immediately of the disaster recovery declaration:

1. *Senior Staff Member*
2. *Disaster Recovery Team*
3. *Disaster Recovery Site Provider*

3.5 Notification Procedures

Define how and when IT management, the Emergency Management Response Team, and DR Team Members will be notified. Identify what information and/or instructions will be provided at each level of notification.

3.6 Recovery Procedures

The following table provides sample recovery procedures.

Topic	Description
Backup Tapes and Offsite Storage	*Describe backup process and frequency.* • *Define offsite storage locations and recall procedures, e.g., vendor contacts, delivery locations*
Computer Recovery	*Document mainframe setup.* • *Document recovery process, e.g., restore backup tape, DASD restore & cataloging, TCP/IP modifications.*
Server Recovery	• *Describe the LAN topology and protocols used (e.g., Ethernet, ATM).* • *Provide LAN production structures and recovery locations.* • *Provide system configurations, vendors, and their contact data.* • *Provide a procedures checklist on how servers will be configured, validated, loaded, etc.*
Web Support	• *Provide Web Site information, e.g., hardware, software, and configurations used to create and host the web site.* • *Review website to ensure hard-coded IP addresses, domain names, or drive letters to reduce system recovery implementation time.* • *Ensure Security Policies and Controls are maintained.* • *Modify DNS server names providing URL mappings to IP addresses*

Topic	Description
	when necessary.

4 Technology Infrastructure Recovery Plan Samples

4.1 Network Recovery Plan

Prerequisites

- ***Frame relay network installed at disaster recovery site.***

Action Item	Description	Responsibility
Disconnect Company Primary Router	*Telnet to primary router*	*Network Administrator or Disaster Recovery Company*
Disconnect Company Secondary Router	*Telnet to backup router*	*Network Administrator or Disaster Recovery Company*
Configure Disaster Recovery Network as the Company Network	*Telnet to internet address*	*Disaster Recovery Company*

4.1.1 Network Testing

Sample Test Plan Steps

Test Item	Description
Internal Network Addressing Test	*From a computer on the disaster recovery site network, ping servers TCP/IP address at various locations and multiple disaster recovery site servers to ensure network connectivity is established correctly.*
Internal Network Name Test	*From a computer on the disaster recovery site, ping network server names to ensure internal DNS servers are functioning properly. Perform a trace route to ensure proper network routing and naming.*
Internal Network Browsing Test	*Browse the internal network to ensure Windows browsing is functioning properly. Perform a trace route to ensure proper network routing and naming.*

4.2 Windows Server Recovery Plan

Prerequisites

- *Network installed at disaster recovery site*
- *Domain controller at disaster recovery site*

Action Item	Description	Team Member Responsibility
Reconfigure Domain Replication	*DNS Configuration – Change domain to point to itself.* *Use Sites and Services to reconfigure domain at the replication hub.* *Modify WINS to replicate to all domain controllers.* *Size disaster recovery domain controllers.*	*Technology Infrastructure Manager*
File Server Renaming	*Rename Windows file servers at the disaster recovery site to production server names.*	*Technology Infrastructure Manager*
Print Serving	*Setup acquired printers in the event of an emergency.*	*Technology Infrastructure Manager*

4.2.1 Windows Server Testing

Sample Test Plan Steps

Test Item	Description
Windows File Sharing	*Verify access thru the Windows Run window or Windows Explorer.*
Test Replication	*Verify changes made on the disaster recovery domain controllers are being replicated to at least three domain controllers.*
Printer Test	*Print to test printer at the disaster recovery site.*

4.3 Electronic Mail Recovery Plan

Prerequisites

- *Network Installed at Disaster Recovery Site*
- *Windows Server Recovery - Active Directory domain controller(s) and global catalog server(s) names, domain administrator account, and password.*
- *Replacement hardware and component device drivers are disk mirror compatible.*
- *Disk mirror of the operation system and exchange program files from the production system.*
- *Backups of exchange databases.*
- *Exchange master administrator account name and password.*
- *IP addressing information of new environment (if applicable).*

Action Item	Description	Responsibility
Recover the operating system, exchange program files, and disk arrays.	*Recover the operating system, exchange program files, and recreate the disk arrays to prepare for database restore. Perform this for all exchange servers that have production mailbox stores:* • *Operating system and exchange program files* • *Disk arrays*	
Registry changes	*Perform registry changes to make exchange aware of new domain controllers and global catalog servers if they are not present in the recovery environment.*	
Exchange services and attributes	*Verify the exchange services start, e.g.,* • *Microsoft Exchange System Attendant* • *Microsoft Exchange Information Store*	
Drive letters	*Verify drive letters are correct and attached.* • *Operating system* • *Transaction logs* • *Mailbox stores* • *Computer DVD / CD-ROM*	
Exchange Access information	*Update Exchange Access information with new Domain Controller(s) and Global Catalog server(s) information.*	
Recipient Update Service Domain Controller	*Modify the Recipient Update Service Domain Controller.*	

Action Item	Description	Responsibility
Exchange Folder Structure	*Update the exchange folder structure (e.g., create directories-transaction log) and create blank mailbox stores with drives based on database paths reflected in System Manager.*	
Exchange restore and mounting process	• *Change the restore status of all stores to be restored and dismounted.* • *Restore Exchange Databases from backup using Backup Exec.* • *Mount databases after the restore.*	
Outlook Web Access	*Perform configuration changes needed for Outlook Web Access (OWA) server(s).*	

4.3.1 Electronic Mail Testing

Sample Test Plan Steps

Test Item	Description
Outlook Web Access	*Using Outlook Web Access (OWA), start Internet Explorer and go to company's OWA address at https://webmail.companyname.com.*
Logon	*Logon using your network ID and password.*
Inbox Messages	*Verify that messages displayed in your Inbox are current or as of the restored backup period.*
Send Mail1	*Send mail to an Internet account that you have access to. Verify that it was received in this Internet mailbox.*
Send Mail2	*Send mail from your Internet account to your account. Verify that it was received in your mailbox.*

4.4 Telecommunications Recovery Plan

Prerequisites

- *Office space setup completed with telephone handsets.*

Action Item	Description	Responsibility
Number Redirection	*Inform the local exchange provider to forward company telephone numbers to numbers assigned at the disaster recovery site.*	*Communications Manager*
Handset Setup	*Provide to Disaster Recovery Company the MAC addresses of any additional phone handsets they wish to use (with usernames assigned to each phone).*	*Communications Manager*
Site Setup	*Implement final configuration steps for Call Manager services at the disaster recovery site.*	*Disaster Recovery Company*
Voice Mail	*Setup voice mail on the company's Call Manager.*	*Disaster Recovery Company*
Voice Recording	*Implement a voice recording on the company's Call Manager at the DR site.*	*Communications Manager*

4.4.1 Telecommunications Testing

Sample Test Plan Steps

Test Item	Description
Internal Calling	*Make an IP Phone to IP Phone call from one number at the disaster recovery site to another number at the disaster recovery site.*
External Calling	*Make a local phone call to a number outside of the building, 10 digit dialing (include area code) is required. Also from an external phone make a call into the disaster recovery site to make sure the site is able to receive external calls and test the number transfer service.*
International & Long Distance	*Make both a long distance and international call.*
Voice Mail	*Check if voice mail is functional. From another phone leave a message at your number to check the message waiting light.*

4.5 Applications Infrastructure

Provide a recovery plan and test plan steps for major applications, e.g.,

- ***Financials***
- ***Payroll & Human Resources***
- ***Treasury***
- ***Tax***
- ***Marketing Database***
- ***Time Entry.***

5 Training and Documentation Requirements

Provide training and documentation information that is required to support the disaster recovery process, applications, system, operations or services., training plans, training materials, support documentation, and user documentation.

Training / Documentation	Resource	Schedule	Comments

6 Glossary

List any document terms that may not be fully understood without some explanation.

Term	Definition
Disaster recovery	Disaster recovery is the process whereby a company would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
Disaster Recovery Plan	A disaster recovery plan is part of an overall contingency plan to complete that restoration task and keep the company running. A disaster recovery plan is required for any publicly traded company and companies that need to minimize loss. This disaster recovery declaration plan is designed for conditions under which the company site is unable to function under standard daily business procedures.

7 APPENDIX

7.1 Executive Sponsors

Last Name	First Name	Application Name

7.2 User Information

Last Name	First Name	Dept.	DR Rep	Application Name	Purpose

7.3 Applications

Dept	Application Name	Purpose	Priority Ranking		Manager	Location	Primary and Secondary IT Contacts	Primary and Secondary Functional Contacts
			1	< 8 hours				
			2	24 hours				
			3	48 hours				
			4	72+ hours				
			5	3-5 days				
			6	>5 days				

7.4 Equipment Inventory

Equipment Type	ID	Model	Service	IP Address
Server	*XYZ1*	*Compaq DL380*	*File Server*	*xx.xx.xxx.xxx*
Telephone	*1*	*Cisco 7960*		

7.5 Production Site Data Communications Configuration

ID	Description	Bandwidth	Vendor / Contact Agency / Person	Contact #s	Date Last Tested

7.6 Recovery Site(s) Data Communications Configuration

ID	Description	Bandwidth	Vendor / Contact Agency / Person	Contact #s	Date Last Tested

7.7 Data Communications Equipment

Device Type	Description	Serial Number	Contact Agency / Person	Date Last Tested / By Whom
Routers				
Switches				

7.8 Network Diagram-Sample