Disaster Recovery and Business Continuity Plan

If you are reading this document it means that a critical situation has occurred that is either a disaster or could potentially escalate to a disaster. In which case, this plan must be initiated. Please go to the section entitled:

3.1 Call Matrix

Table of Contents

Table of Contents 3

Document Revision History 4

Chapter 1: Overview 5

1.1 Distribution List 5

1.2 Document Location 5

1.3 DR Plan Maintenance Cycle 6

1.4 Purpose 7

1.5 Scope 7

1.6 Objectives 8

1.7 Definitions 9

Chapter 2: Recovery Procedures 10

2.1 Summary of Recovery Procedures 10

Chapter 3: Team Descriptions 11

3.1 Call Matrix 11

3.2 Disaster Recovery Management Team 12

3.3 Disaster Recovery Technical Team 12

3.4 Disaster Recovery Organization Chart 13

3.5 Roles and Responsibilities 13

DR Management Team 13

Information Security Office Team 13

DR Coordinator 13

DR Crisis Manager 14

Chapter 4: Teams and Members 15

4.1 Key Contacts Chart: 15

Chapter 5: Locations 16

5.1 Disaster Recovery Command Centre 16

Contingency Location Usage 16

Command Centre 16

Production Site 16

Recovery Site 16

Chapter 6: [Company] Acceptance and Sign-off 17

Chapter 7: Appendix Telephone Log 18

Document Revision History

Date	Version	Author	Comments

Chapter 1: Overview

1.1 Distribution List

It is crucial that each team member involved in this plan maintain an up to date hard copy of this document. In a disaster situation chances are that soft copies will not be accessible.

This document must be distributed as follows:

- A soft copy maintained at [a link to a secure online source], with all other related materials.
- A hard copy and soft copy for each Team Member described in section 3.
- A hard copy and soft copy maintained at [Company] facility

1.2 Document Location

This document is stored at the following locations:

Location 1:
[COMPANY]
[COMPANY address]
[COMPANY phone number]

Location 2:
[COMPANY] (
[COMPANY address]
[COMPANY phone number]

Location 3:
[COMPANY]
[COMPANY address]
[COMPANY phone number]

1.3 DR Plan Maintenance Cycle

The Disaster Recovery (DR) plan of [Company's] Mission Critical applications is supported by this master plan. In addition, a set of supporting documents and logs are in place in order to provide reporting after the DR process. These documents include: DR Problem Log, DR Timeline and DR Executive Summary.

Necessary Standard Operational Procedures (SOPs) that will eventually need to be followed are also listed below. These documents must be kept up-to-date by their respective owners.

Document	Owner	Review period	Document location
MASTER PLAN	Title/Team/Individual 1	**-Whenever significant changes are made in any of the following areas: strategy, personnel, hardware, software, links, etc.** **-After every Drill (at least twice a year)**	[soft copy location path 1] [hard copy location]
[SOP1]	Title/Team/Individual 2		[soft copy location path 2] [hard copy location]
[SOP 2]	Title/Team/Individual 3		[soft copy location path 3] [hard copy location]
DR PROBLEM LOG	Title/Team/Individual 4		[soft copy location path 4] [hard copy location]
DR TIMELINE	Title/Team/Individual 5		[soft copy location path 5] [hard copy location]
DR EXECUTIVE SUMMARY	Title/Team/Individual 6		[soft copy location path 6] [hard copy location]

Specific Standard Operational Procedures (SOPs) may be obtained by SERVICE PROVIDER or developed internally by [COMPANY].

1.4 Purpose

The document aims to put procedures in place in order to successfully recover Mission Critical Applications after any disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:

- Notification/Activation Phase – Activating the plan.
- Recovery Phase – Restoring temporary operations and recovering any damages that may have occurred to the original system.

- Identify activities, resources, and procedures needed to carry out all [COMPANY] processing requirements during interruptions to normal business operations.

- Assign responsibilities to the designated [COMPANY] authorized representative in addition to providing guidance in the recovery of IT assets during periods of interruption to normal operations.

- Ensure coordination and communication between the participants at service providers and [COMPANY] who have been assigned to the recovery planning strategy. Ensure coordination with external points of contact and vendors who will participate in the recovery planning strategy.

1.5 Scope

When developing [Company's] Disaster Recovery Plan, the following assumptions were utilized:

- [assumption 1]

- [assumption 2]

The [Companys] Disaster Recovery Plan does not apply to the following situations:

- [exception 1]

- [exception 2]

1.6 Objectives

The objectives of this plan are:

[select objectives from the list provided below]

- Minimize economic loss
- Establish a solid communication matrix to be used in the event of disaster
- Reduce disruptions to operations
- Provide organizational stability
- Achieve orderly recovery
- Reduce legal liability
- Limit potential exposure
- Lower probability of occurrence
- Reduce reliance on key personnel
- Protect assets
- Minimize decision making during disaster
- Reduce delays in critical recovery situations
- Provide a sense of security
- Comply with regulatory requirements
- Recover all Mission Critical applications within the defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

According to the Business Impact Analysis (BIA), the following applications were identified as Mission Critical requiring a Disaster Recovery plan:

Application	Module	Server	Database	RTO	RPO
[application 1]					
[application 2]					

The Disaster Recovery Plan is intended to:

- Ensure that all known and available resources will be used to recover business functions following an emergency or disaster event that could impact the operation of mission critical systems.
- Provide a set of actionable procedures to restore prioritized business processes with maximum speed and minimum impact to internal and external customers.

The following network sites are attended by this Disaster Recovery Plan:

- Site 1:
- **[COMPANY] ([COMPANY])**
- [COMPANY address]
- [COMPANY phone number]

- Site 2:
- **[COMPANY] ([COMPANY])**
- [COMPANY address]
- [COMPANY phone number]

1.7 Definitions

A **Disaster,** for the purposes of this plan, is **ANY** event that results in the specified Mission Critical application systems (defined in section 1.7) being unavailable for a period of time in excess of [x hours/days].

This could be an event of significant magnitude that threatens the continued stability and/or continuance of an institution, that brings about great loss and/or damage, or that creates an inability on the organization's part to perform critical functions.

It is important to highlight that not all incidents will result in initiating the DR process. Therefore, necessary steps must be taken to assess the severity of the incident prior to declaration.

An incident is defined as any unexpected event that may or may not cause a system to function improperly.

A critical incident is any event that results in the impairment of business critical functions, leaving [COMPANY] unable to provide essential services for a period of time in excess of [x hours/days]. Incidents may be internal or external to business operations.

Chapter 2: Recovery Procedures

2.1 Summary of Recovery Procedures

In the event of a critical incident that causes the DR process to be initiated, the Recovery Teams will recover the applications and data according to the documented Standard Operational Procedures (SOPs are not in the scope of this document).

The chart below may be used to identify key [COMPANY] SOPs when addressing a disaster recovery situation.

SOP	Description	Responsible Person/Department

Backups for Mission Critical applications are executed in accordance with the schedule below:

[MC application 1: example]

[Backup Oracle] – [incremental] daily
[Backup Unix] – [incremental] weekly (Wednesday)
[Backup Windows] – [incremental] weekly (Tuesday)

[MC application 2: example]

[Backup Oracle] – [incremental] daily
[Backup Unix] – [incremental] weekly (Wednesday)
[Backup Windows] – [incremental] weekly (Tuesday)

The following network diagram represents the Infrastructure including key connections, servers and critical applications.

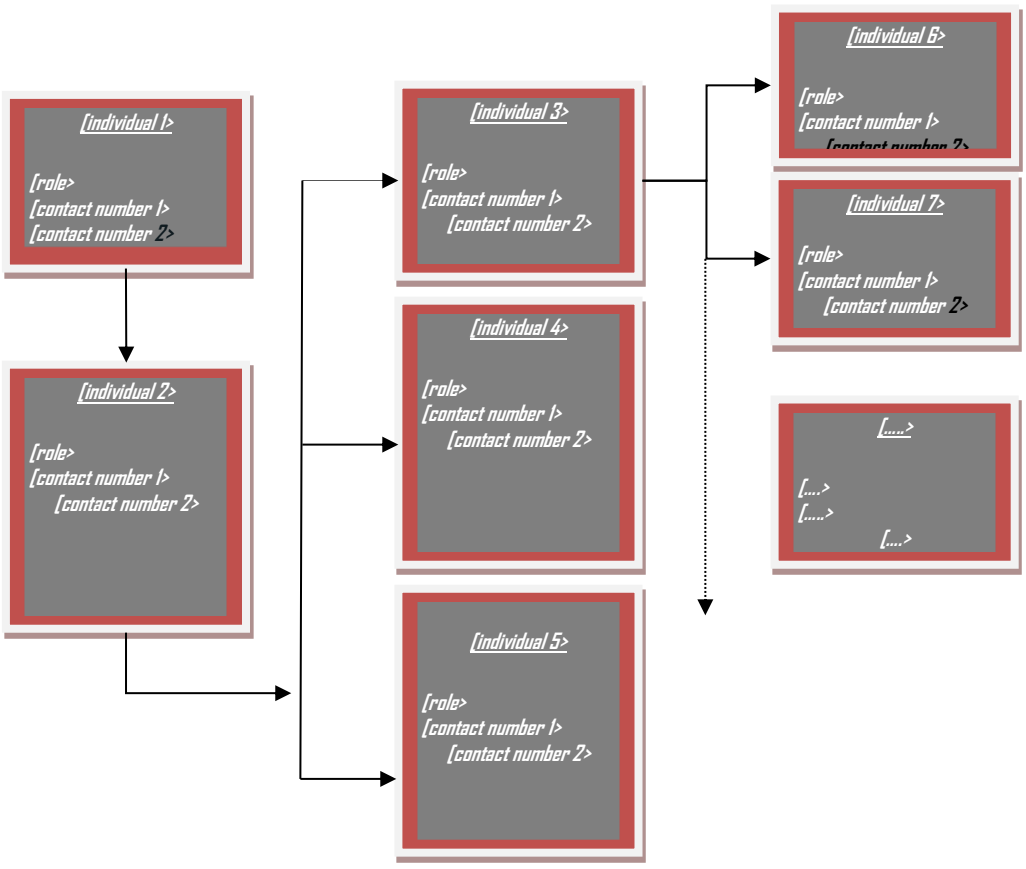
[insert network diagram here]

Chapter 3: Team Descriptions

3.1 Call Matrix

The following call matrix will be used to activate the Disaster Recovery Team:

- Names in red must have priority when being contacted.
- Use the table in Chapter 7 to log the call matrix process.



3.2 Disaster Recovery Management Team

A permanent Management Team is responsible for overseeing recovery operations. This Team will be informed when a disaster occurs and will be comprised of the following staff:

- [team/individual 1]
- [team/individual 2]
- [team/individual 3]

In the event of any of the above personnel being unavailable, their nominated deputies will stand in. Depending on the type of the disaster, the Management Team will co-opt additional members.

The team will be responsible for assessing the extent of the disaster as well as directing and coordinating recovery activities involving other parties as necessary.

They will also assess the severity of the disaster, and determine whether the full Disaster Recovery response is required.

3.3 Disaster Recovery Technical Team

A dedicated Technical Team of experienced staff will be formed to implement the recovery process under the direction of the following DR Coordinators:

- [COMPANY] DR Coordinator
- Information Security Office Team
- [COMPANY] DR Crisis Manager

The major responsibilities of the technical team are:

- Determine the effects of the Disaster on technical systems.
- Establish the activities required to recover the systems and data, whether at the production site or Disaster Recovery site.
- Implement recovery procedures and complete them as quickly as possible.
- Notify, involve and work with Systems Managers to re-establish customer processing.
- Report to the Management Team on progress and recovery status.

3.4 Disaster Recovery Organization Chart

[Insert an organization chart containing names and roles here]

3.5 Roles and Responsibilities

DR Management Team

- Make the decision to declare a Disaster.
- Manage and coordinate the Disaster Recovery Plan.
- Authorize and direct the activation of the required Disaster Recovery Management Teams.
- Authorize as required the notification of the alternate processing facilities and sites.
- Review the recovery procedures to be activated in order to support the recovery objectives.
- Direct the Disaster Recovery Team Leaders to identify the priority in which the other personnel should be alerted. The following is to be Considered:
  - Personnel needed by various teams to meet recovery objectives
  - Additional personnel needed immediately
  - Personnel that should stay home on standby

Information Security Office Team

- Review the recovery goals.
- Request support based on the extent of damage.
- Support Disaster Recovery Team to ensure the Information Security procedures are followed.
- Assist DR Crisis Manager and DR Coordinator with the preparation of a news media statement. Provide the following information:
  - A description of the incident.
  - How did it happen?
  - When did it happen?
  - Were there any injuries? How serious?
  - Where has the injured person(s) been taken (hospital, location)?
  - Has the family been notified?
  - How serious was the incident in terms of equipment loss, damage to software, total dollar loss, etc.?
  - Will this incident cause any difficulty for]COMPANY] in the short term?

DR Coordinator

- Coordinate [COMPANY] DR teams to provide required network, server, database, and storage infrastructure to support critical applications during the DR process.

- Establish a schedule for status reports on:
  - Completion of system restoration
  - Accessibility of an alternate-processing site
  - Data synchronization and problem reporting
- Schedule continued status reporting

DR Crisis Manager

- [COMPANY] DR Crisis Manager's first priority is to keep the customer fully informed at all times and to provide a single point of contact for the customer to reach the Disaster Recovery Teams.

[COMPANY] DR Crisis Manager ensures all users and clients are familiar with the Recovery Management plan.

* Keep your own copy of these recovery procedures, along with your employee identification, on your person.
* Determine if any additional telephones will be required for auxiliary staffing.
* Obtain the status of operations and processing at the time of the disruption from the Information Security Office Team. This includes:
  - General status of customer data and information
  - Anticipated time without operating and processing services
  - Availability of the next status update
* Develop a suggested statement to be given to users, clients and media during the initial contact. Obtain approval from the Disaster Response Management Team. The statement should include:
  - A brief description of the Disaster situation
  - An estimate of when services will be available to users/clients, and what level of service will be provided
  - A request that they alert all personnel affected in their group
  - Assurance that users/clients will be notified in the event of any change in recovery status
* After the Disaster Recovery operation is officially concluded, prepare a statement to be given to users, clients and media if necessary.

Chapter 4: Teams and Members

4.1 Key Contacts Chart:

This section contains a full description of the various teams' contact information. The following tables can be used in case any primary contacts in the Call Matrix cannot be located.

DR Management Team					
Name	**Title**	**Work Phone**	**Mobile Phone**	**Home Phone**	**e-mail**
Name 1	Title 1	Work Phone 1	Mobile Phone 1	Home phone 1	email 1
Name 2	Title 2	Work Phone 2	Mobile Phone 2	Home phone 2	email 2
Name 3	Title 3	Work Phone 3	Mobile Phone 3	Home phone 3	email 3
Name 4	Title 4	Work Phone 4	Mobile Phone 4	Home phone 4	email 4

Information Security Office Team					
Name	**Title**	**Work Phone**	**Mobile Phone**	**Home Phone**	**e-mail**
Name 1	Title 1	Work Phone 1	Mobile Phone 1	Home phone 1	email 1
Name 2	Title 2	Work Phone 2	Mobile Phone 2	Home phone 2	email 2
Name 3	Title 3	Work Phone 3	Mobile Phone 3	Home phone 3	email 3
Name 4	Title 4	Work Phone 4	Mobile Phone 4	Home phone 4	email 4

DR Coordinator					
Name	**Title**	**Work Phone**	**Mobile Phone**	**Home Phone**	**e-mail**
Name 1	Title 1	Work Phone 1	Mobile Phone 1	Home phone 1	email 1

DR Crisis Manager					
Name	**Title**	**Work Phone**	**Mobile Phone**	**Home Phone**	**e-mail**
Name 1	Title 1	Work Phone 1	Mobile Phone 1	Home phone 1	email 1

Chapter 5: Locations

5.1 Disaster Recovery Command Center

A Command Center will be established to direct business continuity efforts. This will be the default meeting point for all DR processes.

- Primary Command Center: [site 1]

Contingency Location Usage

The following sites will be used to execute this plan:

Command Center

Sub location:	**Location Phone:**
[Site 1]	**[Phone]**

Fax:
Location Address:
City:
State:
Zip:
Country:
Comments:

Production Site

Sub location:	**Location Phone:**
[Site 2]	**[Phone]**

Fax:
Location Address:
City:
State:
Zip:
Country:
Comments:

Recovery Site

Sub llocation:	**Location Phone:**
[Site 1]	**[Phone]**

Fax:
Location Address:
City:
State:
Zip:
Country:

Comments:

Chapter 6: [Company] Acceptance and Sign-off

[COMPANY] Managers are responsible for the accuracy of the information contained in the Master Plan document. It is [COMPANY] Managers' responsibility to notify the appropriate parties of any changes or additions to this document.

I agree that the information contained in the Master Plan is accurate and complete.

Name	Title	Date	Signature
[customer manager 1]			
[customer manager 2]			
[customer manager 3]			

Remarks:

.....
.....
.....
.....
.....
.....
.....
.....

Chapter 7: Appendix

Telephone Log

The form on the following page should be used to record all outbound call attempts during the initial notification process, and for all other outbound calls.

TELEPHONE LOG								
Contacted by:				**Date:**				**Time:**
Caller name:				**Calling Results**				**Comments**
Date	**Time**	**Name**	**Phone #**	**Reached**	**N/A**	**No Answer**	**Busy**	**Left message, Not in service, Answering machine, Given new number, etc.**