# Disaster Recovery Plan Template

**ITA – Premium: Strategy & Planning Tool**

## Introduction: How to Use This Tool

Disaster Recovery Plans (DRP) are complex documents that contain a wealth of information about the IT operations of an enterprise and yet must present that information in a format that is easily consumable during an actual emergency. This template is one example of how to capture and organize the necessary information to ensure that the enterprise is in a position to survive if a disaster occurs.

Please note, this template is meant as a guide only. Enterprises using this template should review it carefully to determine whether it fits their needs and should customize it to best meet their own needs and goals.

This template contains instructional text (presented as grey-highlighted black text such as this). Please review all instructional text to ensure complete understanding of the purpose of each document section and follow those instructions to complete the section in question. This template also contains example text (*presented as italicized grey text, such as this).* These examples exist to provide guidance as to how to complete a section and supplement the information provided in the instructional text. In some cases example text (e.g. bullet lists) may be used as-is, added to, or deleted from while in other cases (e.g. sample table entries) it should be replaced with accurate, enterprise specific information.

All attempts have been made to make this template as complete as possible. As a result, some enterprises may find that the document is more thorough than required. In those circumstances it is entirely appropriate to delete entire sections that have been deemed unnecessary. Info-Tech has attempted to provide guidance as to which sections most likely need to be retained versus those that can be eliminated with the following color-coded text:

**Mandatory** – it is likely that all enterprises will need to complete this section.

**Elective** – it is possible that only some enterprises will need to complete this section.

Finally, this template also includes markers where the enterprise may wish to use a *Find and Replace* function to insert the name of the company, the name of partner companies and other such information. These fields are delineated with double angle brackets (such as **<<this>>**). Performing a *Find and Replace* on these terms can expedite the process of completing the template.

## Instructions

Complete all required sections and delete all unnecessary sections, replacing example text and *Find and Replace* text during the process. Upon completion of all sections, delete all instructional text (including this instruction page) as well as all Mandatory/Elective markers and *Find and Replace* markers. Update the Table of Contents (right click and select "Update Fields") and then publish.

Once this document is completed in full, provide hard-copies to all stakeholders and all employees with DR responsibilities. Create additional hard-copies as well as soft copies for each data center or facility that houses IT systems (including and standby or recovery facilities that may exist).

Ensure the access to these hard and soft copies is protected to ensure the integrity of the document.

Finally, review and revise the document on a regular basis to ensure continued applicability, revising as required.

<<Organization Name>> Disaster Recovery Plan

Date

Version 1

# Disaster Recovery Plan Template
**ITA – Premium: Strategy & Planning Tool**

## Table of Contents

# Introduction

## Mandatory

This Disaster Recovery Plan (DRP) captures, in a single repository, all of the information that describes <<Organization's Name>>'s ability to withstand a disaster as well as the processes that must be followed to achieve disaster recovery.

This section should be completed by all organizations. It helps position the DRP, detailing what is included in the plan and what areas are addressed. Edit this section to suit your organization's needs, lists and paragraphs should be made relevant to your organization.

# Definition of a Disaster

## Elective

A disaster can be caused by man or nature and results in <<Organization Name>>'s IT department not being able to perform all or some of their regular roles and responsibilities for a period of time.  <<Organization Name>> defines disasters as the following:

- Edit this list to reflect your organization
- *One or more vital systems are non-functional*
- *The building is not available for an extended period of time but all systems are functional within it*
- *The building is available but all systems are non-functional*
- *The building and all systems are non functional*

The following events can result in a disaster, requiring this Disaster Recovery document to be activated:

- Edit this list to reflect your organization
- *Fire*
- *Flash flood*
- *Pandemic*
- *Power Outage*
- *War*
- *Theft*
- *Terrorist Attack*

# Purpose

## Mandatory

The purpose of this DRP document is twofold: first to capture all of the information relevant to the enterprise's ability to withstand a disaster, and second to document the steps that the enterprise will follow if a disaster occurs.

Note that in the event of a disaster the first priority of <<Organization Name>> is to prevent the loss of life. Before any secondary measures are undertaken, <<Organization Name>> will ensure that all employees, and any other individuals on the organization's premises, are safe and secure.

After all individuals have been brought to safety, the next goal of <<Organization Name>> will be to enact the steps outlined in this DRP to bring all of the organization's groups and departments back to business-as-usual as quickly as possible. This includes:

- Edit this list to reflect your organization
- *Preventing the loss of the organization's resources such as hardware, data and physical IT assets*
- *Minimizing downtime related to IT*
- *Keeping the business running in the event of a disaster*

This DRP document will also detail how this document is to be maintained and tested.

## Scope

### Mandatory

The <<Organization Name>> DRP takes all of the following areas into consideration:

- Edit this list to reflect your organization
- *Network Infrastructure*
- *Servers Infrastructure*
- *Telephony System*
- *Data Storage and Backup Systems*
- *Data Output Devices*
- *End-user Computers*
- *Organizational Software Systems*
- *Database Systems*
- *IT Documentation*

This DRP does not take into consideration any non-IT, personnel, Human Resources and real estate related disasters. For any disasters that are not addressed in this document, please refer to the business continuity plan created by <<Organization Name>> or contact <<Business Continuity Lead>> at <<Business Continuity Lead Contact Information>>.

## Version Information & Changes

### Mandatory

Any changes, edits and updates made to the DRP will be recorded in here. It is the responsibility of the Disaster Recovery Lead to ensure that all existing copies of the DRP are up to date. Whenever there is an update to the DRP, <<Organization Name>> requires that the version number be updated to indicate this.

Add rows as required as the DR Plan is amended.

| Name of Person Making Change | Role of Person Making Change | Date of Change | Version Number | Notes |
|---|---|---|---|---|
| *John Smith* | *DR Lead* | *01/01/09* | *1.0* | *Initial version of DR Plan* |
| *John Smith* | *DR Lead* | *01/01/10* | *2.0* | *Revised to include new standby facilities* |
| *Fred Jones* | *CEO* | *01/03/10* | *2.1* | *Replaced John Smith as DR Lead* |
| | | | | |
| | | | | |

## Disaster Recovery Teams & Responsibilities

### Mandatory

In the event of a disaster, different groups will be required to assist the IT department in their effort to restore normal functionality to the employees of <<Organization Name>>. The different groups and their responsibilities are as follows:

- Edit this list to reflect your organization
- *Disaster Recovery Lead(s)*
- *Disaster Management Team*
- *Facilities Team*
- *Network Team*
- *Server Team*
- *Applications Team*
- *Operations Team*
- *Management Team*
- *Communications Team*
- *Finance Team*

The lists of roles and responsibilities in this section have been created by <<Organization Name>> and reflect the likely tasks that team members will have to perform. Disaster Recovery Team members will be responsible for performing all of the tasks below. In some disaster situations, Disaster Recovery Team members will be called upon to perform tasks not described in this section.

Please note that the following teams will vary depending on the size of your organization. Some teams/roles may be combined or may be split into more than one team.

## Disaster Recovery Lead

### Mandatory

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs at <<Organization Name>>, regardless of their department and existing managers. All efforts will be made to ensure that this person be separate from the rest of the disaster management teams to keep his/her decisions unbiased; the Disaster Recovery Lead will not be a member of other Disaster Recovery groups in <<Organization Name>>.

### Role and Responsibilities

- Edit this list to reflect your organization
- *Make the determination that a disaster has occurred and trigger the DRP and related processes.*
- *Initiate the DR Call Tree.*
- *Be the single point of contact for and oversee all of the DR Teams.*
- *Organize and chair regular meetings of the DR Team leads throughout the disaster.*
- *Present to the Management Team on the state of the disaster and the decisions that need to be made.*
- *Organize, supervise and manage all DRP test and author all DRP updates.*

### Contact Information

Add or delete rows to reflect the size the Disaster Recovery Team in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|------|-----------|-------------------|-------------------|---------------------|
| *John Smith* | *Primary Disaster Lead* | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| *Fred Jones* | *Secondary Disaster Lead* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Disaster Management Team

### Elective

The Disaster Management Team that will oversee the entire disaster recovery process. They will be the first team that will need to take action in the event of a disaster. This team will evaluate the disaster and will determine what steps need to be taken to get the organization back to business as usual.

Please note than in a small organization, these roles may be performed by the Disaster Recovery Lead.

### Role & Responsibilities

- Edit this list to reflect your organization
- *Set the DRP into motion after the Disaster Recovery Lead has declared a disaster*
- *Determine the magnitude and class of the disaster*
- *Determine what systems and processes have been affected by the disaster*
- *Communicate the disaster to the other disaster recovery teams*
- *Determine what first steps need to be taken by the disaster recovery teams*
- *Keep the disaster recovery teams on track with pre-determined expectations and goals*
- *Keep a record of money spent during the disaster recovery process*
- *Ensure that all decisions made abide by the DRP and policies set by <<Organization Name>>*
- *Get the secondary site ready to restore business operations*
- *Ensure that the secondary site is fully functional and secure*
- *Create a detailed report of all the steps undertaken in the disaster recovery process*
- *Notify the relevant parties once the disaster is over and normal business functionality has been restored*
- *After <<Organization Name>> is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

### Contact Information

Add or delete rows to reflect the size the Disaster Management Team in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|------|-----------|-------------------|-------------------|---------------------|
| *John Smith* | *"Normal" title* | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| *Fred Jones* | *"Normal" title* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Facilities Team
### Mandatory
The Facilities Team will be responsible for all issues related to the physical facilities that house IT systems. They are the team that will be responsible for ensuring that the standby facilities are maintained appropriately and for assessing the damage too and overseeing the repairs to the primary location in the event of the primary location's destruction or damage.

## Role & Responsibilities
- Edit this list to reflect your organization
- *Ensure that the standby facility is maintained in working order*
- *Ensure that transportation is provided for all employees working out of the standby facility*
- *Ensure that hotels or other sleeping are arranged for all employees working out of the standby facility*
- *Ensure that sufficient food, drink, and other supplies are provided for all employees working out of the standby facility*
- *Assess, or participate in the assessment of, any physical damage to the primary facility*
- *Ensure that measures are taken to prevent further damage to the primary facility*
- *Work with insurance company in the event of damage, destruction or losses to any assets owned by <<Organization Name>>*
- *Ensure that appropriate resources are provisioned to rebuild or repair the main facilities in the event that they are destroyed or damaged*
- *After <<Organization Name>> is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

## Contact Information
Add or delete rows to reflect the size of the Facilities Team in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|---|---|---|---|---|
| *John Smith* | *VP Facilities* | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| *Fred Jones* | *Standby Facility Manager* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Network Team

### Mandatory

The Network Team will be responsible for assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the enterprise as well as telephony and data connections with the outside world. They will be primarily responsible for providing baseline network functionality and may assist other IT DR Teams as required.

### Role & Responsibilities

- Edit this list to reflect your organization
- *In the event of a disaster that does not require migration to standby facilities, the team will determine which network services are not functioning at the primary facility*
- *If multiple network services are impacted, the team will prioritize the recovery of services in the manner and order that has the least business impact.*
- *If network services are provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.*
- *In the event of a disaster that does require migration to standby facilities the team will ensure that all network services are brought online at the secondary facility*
- *Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order:*
  - o *All members of the DR Teams*
  - o *All C-level and Executive Staff*
  - o *All IT employees*
  - o *All remaining employees*
- *Install and implement any tools, hardware, software and systems required in the standby facility*
- *Install and implement any tools, hardware, software and systems required in the primary facility*
- *After <<Organization Name>> is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

### Contact Information

Add or delete rows to reflect the size of the Network Team in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|------|-----------|-------------------|-------------------|---------------------|
| *John Smith* | *Network Manager* | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| *Fred Jones* | *Network Administrator* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Server Team

**Mandatory**

The Server Team will be responsible for providing the physical server infrastructure required for the enterprise to run its IT operations and applications in the event of and during a disaster. They will be primarily responsible for providing baseline server functionality and may assist other IT DR Teams as required.

## Role & Responsibilities

- Edit this list to reflect your organization
- *In the event of a disaster that does not require migration to standby facilities, the team will determine which servers are not functioning at the primary facility*
- *If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact. Recovery will include the following tasks:*
  - o *Assess the damage to any servers*
  - o *Restart and refresh servers if necessary*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with system patches*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with application patches*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with data copies*
- *Ensure that the secondary servers located in the standby facility are backed up appropriately*
- *Ensure that all of the servers in the standby facility abide by <<Organization Name>>'s server policy*
- *Install and implement any tools, hardware, and systems required in the standby facility*
- *Install and implement any tools, hardware, and systems required in the primary facility*
- *After <<Organization Name>> is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

## Contact Information

Add or delete rows to reflect the size of the Server Team in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|------|-----------|-------------------|-------------------|---------------------|
| *John Smith* | *Operations Manager* | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| *Fred Jones* | *Systems Administrator* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Applications Team

### Mandatory

The Applications Team will be responsible for ensuring that all enterprise applications operates as required to meet business objectives in the event of and during a disaster. They will be primarily responsible for ensuring and validating appropriate application performance and may assist other IT DR Teams as required.

## Role & Responsibilities

- Edit this list to reflect your organization
- *In the event of a disaster that does not require migration to standby facilities, the team will determine which applications are not functioning at the primary facility*
- *If multiple applications are impacted, the team will prioritize the recovery of applications in the manner and order that has the least business impact. Recovery will include the following tasks:*
  - o *Assess the impact to application processes*
  - o *Restart applications as required*
  - o *Patch, recode or rewrite applications as required*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with application patches*
- *Ensure that secondary servers located in standby facilities are kept up-to-date with data copies*
- *Install and implement any tools, software and patches required in the standby facility*
- *Install and implement any tools, software and patches required in the primary facility*
- *After <<Organization Name>> is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

## Contact Information

Add or delete rows to reflect the size of the Application Team in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|---|---|---|---|---|
| *John Smith* | *Program Manager* | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| *Fred Jones* | *Systems Administrator* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Operations Team

### Mandatory

This team's primary goal will be to provide employees with the tools they need to perform their roles as quickly and efficiently as possible. They will need to provision all <<Organization Name>> employees in the standby facility and those working from home with the tools that their specific role requires.

### Role & Responsibilities

- Edit this list to reflect your organization
- *Maintain lists of all essential supplies that will be required in the event of a disaster*
- *Ensure that these supplies are provisioned appropriately in the event of a disaster*
- *Ensure sufficient spare computers and laptops are on hand so that work is not significantly disrupted in a disaster*
- *Ensure that spare computers and laptops have the required software and patches*
- *Ensure sufficient computer and laptop related supplies such as cables, wireless cards, laptop locks, mice, printers and docking stations are on hand so that work is not significantly disrupted in a disaster*
- *Ensure that all employees that require access to a computer/laptop and other related supplies are provisioned in an appropriate timeframe*
- *If insufficient computers/laptops or related supplies are not available the team will prioritize distribution in the manner and order that has the least business impact*
- *This team will be required to maintain a log of where all of the supplies and equipment were used*
- *After <<Organization Name>> is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

### Contact Information

Add or delete rows to reflect the size of the Operations Team in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|------|-----------|-------------------|-------------------|---------------------|
| *John Smith* | *Helpdesk Manager* | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| *Fred Jones* | *Systems Administrator* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Senior Management Team

**Mandatory**

The Senior Management Team will make any business decisions that are out of scope for the Disaster Recovery Lead. Decisions such as constructing a new data center, relocating the primary site etc. should be make by the Senior Management Team. The Disaster Recovery Lead will ultimately report to this team.

## Role & Responsibilities

- Edit this list to reflect your organization
- *Ensure that the Disaster Recovery Team Lead is help accountable for his/her role*
- *Assist the Disaster Recovery Team Lead in his/her role as required*
- *Make decisions that will impact the company. This can include decisions concerning:*
  - o *Rebuilding of the primary facilities*
  - o *Rebuilding of data centers*
  - o *Significant hardware and software investments and upgrades*
  - o *Other financial and business decisions*

## Contact Information

Add or delete rows to reflect the size of the Management Team in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|------|-----------|-------------------|-------------------|---------------------|
| *John Smith* | *CEO* | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| *Fred Jones* | *COO* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Communication Team

### Elective
This will be the team responsible for all communication during a disaster. Specifically, they will communicate with <<Organization Name>>'s employees, clients, vendors and suppliers, banks, and even the media if required.

### Role & Responsibilities
- Edit this list to reflect your organization
- *Communicate the occurrence of a disaster and the impact of that disaster to all <<Organization Name>>'s employees*
- *Communicate the occurrence of a disaster and the impact of that disaster to authorities, as required*
- *Communicate the occurrence of a disaster and the impact of that disaster to all <<Organization Name>>'s partners*
- *Communicate the occurrence of a disaster and the impact of that disaster to all <<Organization Name>>'s clients*
- *Communicate the occurrence of a disaster and the impact of that disaster to all <<Organization Name>>'s vendors*
- *Communicate the occurrence of a disaster and the impact of that disaster to media contacts, as required*
- *After <<Organization Name>> is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

### Contact Information
Add or delete rows to reflect the size of the Communications Team in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|---|---|---|---|---|
| *John Smith* | *VP HR* | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| *Fred Jones* | *Media Relations* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Finance Team
### Elective
This team will be responsible for ensuring that all of <<Organization Name>>'s finances are dealt with in an appropriate and timely manner in the event of a disaster. The finance team will ensure that there is money available for necessary expenses that may result from a disaster as well as expenses from normal day-to-day business functions.

## Role & Responsibilities
- Edit this list to reflect your organization
- *Ensure there is sufficient cash on-hand or accessible to deal with small-scale expenses caused by the disaster. These can include paying for accommodations and food for DR team members, incremental bills, etc.*
- *Ensure there is sufficient credit available or accessible to deal with large-scale expenses caused by the disaster. These can include paying for new equipment, repairs for primary facilities, etc.*
- *Review and approve Disaster Teams' finances and spending*
- *Ensure that payroll occurs and that employees are paid as normal, where possible*
- *Communicate with creditor to arrange suspension of extensions to scheduled payments, as required*
- *Communicate with banking partners to obtain any materials such as checks, bank books etc. that may need to be replaced as a result of the disaster*

## Contact Information
Add or delete rows to reflect the size of the Finance Team in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|------|-----------|-------------------|-------------------|---------------------|
| *John Smith* | *CFO* | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| *Fred Jones* | *Controller* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Other Organization Specific Teams
### Elective
Specify additional teams as required in your organization.

*Define the team's goals here.*

## Role & Responsibilities
- Edit this list to reflect your organization
- *List of team's roles and responsibilities*

## Contact Information
Add or delete rows to reflect the size of the Other Organization DR Teams in your organization.

| Name | Role/Title | Work Phone Number | Home Phone Number | Mobile Phone Number |
|------|-----------|-------------------|-------------------|---------------------|
| *As Required* | *As Required* | *As Required* | *As Required* | *As Required* |
| *As Required* | *As Required* | *As Required* | *As Required* | *As Required* |

## Disaster Recovery Call Tree

### Mandatory

In a disaster recovery or business continuity emergency, time is of the essence so <<Organization Name>> will make use of a Call Tree to ensure that appropriate individuals are contacted in a timely manner.

- The Disaster Recovery Team Lead calls all Level 1 Members (Blue cells)
- Level 1 members call all Level 2 team members over whom they are responsible (Green cells)
- Level 1 members call all Level 3 team members over whom they are directly responsible (Beige cells)
- Level 2 Members call all Level 3 team members over whom they are responsible (Beige cells)
- In the event a team member is unavailable, the initial caller assumes responsibility for subsequent calls (i.e. if a Level 2 team member is inaccessible, the Level 1 team member directly contacts Level 3 team members).

Add as many levels as you need for your organization.

| Contact | | | Office | Mobile | Home |
|---|---|---|---|---|---|
| DR Lead<br>*John Smith* | | | *111-222-3333* | *111-222-3333* | *111-222-3333* |
| | DR Management Team Lead | | | | |
| | | DR Management Team 1 | | | |
| | | DR Management Team 2 | | | |
| | Facilities Team Lead | | | | |
| | | Facilities Team 1 | | | |
| | Network Team Lead | | | | |
| | LAN Team Lead | | | | |
| | | LAN Team 1 | | | |
| | WAN Team Lead | | | | |

| | | | | |
|---|---|---|---|---|
| | WAN Team 1 | | | |
| Server Team Lead | | | | |
| | Server Type 1 Team Lead | | | |
| | Server Type 1 Team 1 | | | |
| | Server Type 2 Team Lead | | | |
| | Server Type 2 Team 1 | | | |
| Applications Team Lead | | | | |
| | App 1 Team Lead | | | |
| | App1 Team 1 | | | |
| | App 2 Team Lead | | | |
| | App 2 Team 1 | | | |
| Management Team Lead | | | | |
| | Management Team 1 | | | |
| Communications Team Lead | | | | |

| | | | | |
|---|---|---|---|---|
| | Communications Team 1 | | | |
| Finance Team Lead | | | | |
| | Finance Team 1 | | | |

A Disaster Recovery Call Tree Process Flow diagram can help clarify the call process in the event of an emergency. This sample may be used as-is or replaced with a custom flow process.
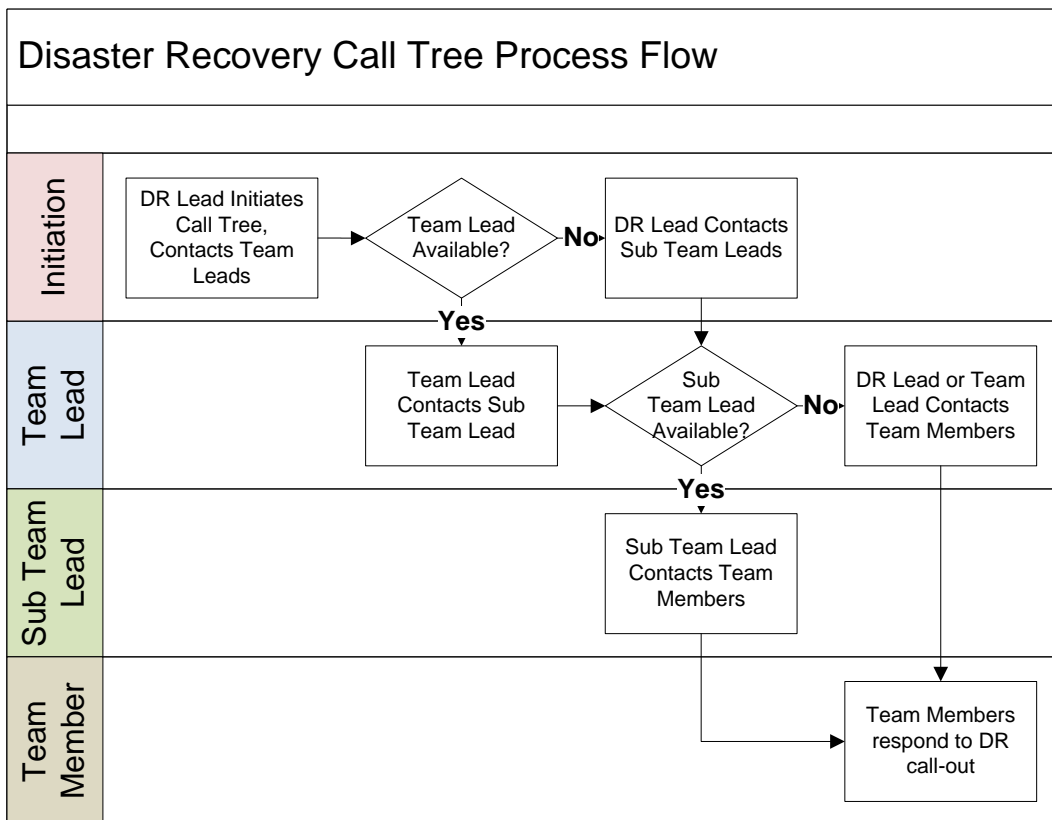
## Disaster Recovery Call Tree Process Flow

| | |
|---|---|
| **Initiation** | DR Lead Initiates Call Tree, Contacts Team Leads → Team Lead Available? —**No**→ DR Lead Contacts Sub Team Leads |
| **Team Lead** | Team Lead Contacts Sub Team Lead → Sub Team Lead Available? —**No**→ DR Lead or Team Lead Contacts Team Members |
| **Sub Team Lead** | Sub Team Lead Contacts Team Members |
| **Team Member** | Team Members respond to DR call-out |

**Yes** (Team Lead Available? → Team Lead Contacts Sub Team Lead)

**Yes** (Sub Team Lead Available? → Sub Team Lead Contacts Team Members)

## Recovery Facilities

**Elective**

In order to ensure that <<Organization *Name*>> is able to withstand a significant outage caused by a disaster, it has provisioned separate dedicated standby facilities. This section of this document describes those facilities and includes operational information should those facilities have to be used.

This section will vary depending on the type of standby facility that your organization uses. Please append this section according to the measures and facilities that your organization has in place. Some organizations may not have a standby facility at their disposal; in this situation, skip this section.

This section is currently populated by an example of a company with a dedicated standby facility.

## Description of Recovery Facilities

**Elective (Mandatory** where facilities exist**)**

The Disaster Command and Control Center or Standby facility will be used after the Disaster Recovery Lead has declared that a disaster has occurred. This location is a separate location to the primary facility. The current facility, located at <<Address of Standby Facility>> is <<standby facility's actual distance away from the primary facility>> miles away from the primary facility.

The standby facility will be used by the IT department and the Disaster Recovery teams; it will function as a central location where all decisions during the disaster will be made. It will also function as a communications hub for <<Organization Name>>.

The standby facility must always have the following resources available:

- Edit this list to reflect your organization
- *Copies of this DRP document*
- *Fully redundant server room*
- *Sufficient servers and storage infrastructure to support enterprise business operations*
- *Office space for DR teams and IT to use in the event of a disaster*
- *External data and voice connectivity*
- *Sleeping quarters for employees that may need to work multiple shifts*
- *Kitchen facilities (including food, kitchen supplies and appliances)*
- *Bathroom facilities (Including toilets, showers, sinks and appropriate supplies)*
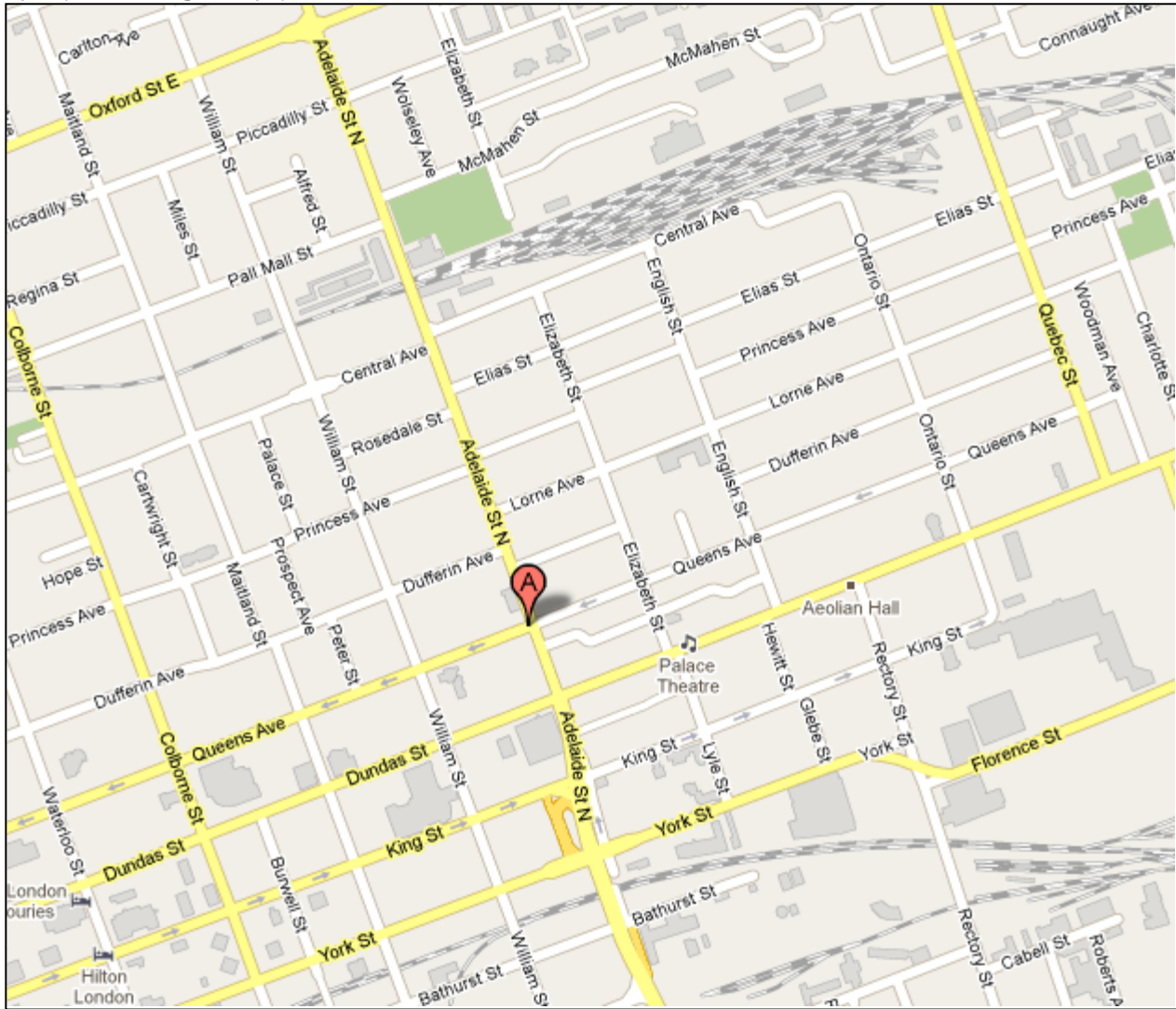- *Parking spaces for employee vehicles*

## Map of Standby Facility Location

Provide a map of the area where the standby facility is located. Use sufficient scale that people can easily determine both where the facility is (not too small a scale) and how to get there (not too large a scale).

*Example (From Google Maps):*



## Directions to Recovery Facility

Provide multiple ways of getting to the facility in the event that one of the roads is unavailable.

<<Directions to the standby facility: Option 1>>

<<Directions to the standby facility: Option 2>>

## Transportation to the Standby Facility

**Elective (Mandatory** where facilities exist**)**
In the event of a disaster, only the Disaster Recovery Teams and select members of the IT department will work out of the standby facility. Since the standby facility is located <<standby facility's actual distance away from the primary facility>> miles away from the primary facility, employees will need to be provided with transportation to the facility if they do not own vehicles or are unable to use them and hotel accommodations if necessary.

Include only those transportation providers that are appropriate given the location of the Standby Facility.

### Taxi Providers

| Taxi Company 1 | |
|---|---|
| Address | |
| Phone Number | |

<<Map of Taxi Company 1's Location>>
<<Directions to get to Rental Car Company 1 from the standby facility>>

| Taxi Company 2 | |
|---|---|
| Address | |
| Phone Number | |

<<Map of Taxi Company 2's Location>>
<<Directions to get to Rental Car Company 1 from the standby facility>>

### Rental Car Providers

| Rental Car Company 1 | |
|---|---|
| Address | |
| Phone Number | |

<<Map of Rental Car Company 1's Location>>
<<Directions to get to Rental Car Company 1 from the standby facility>>

| Rental Car Company 2 | |
|---|---|
| Address | |
| Phone Number | |

<<Map of Rental Car Company 1's Location>>
<<Directions to get to Rental Car Company 1 from the standby facility>>

## Travel Agents (for air or train travel)

| Travel Agent 1 | |
|---|---|
| Address | |
| Phone Number | |

<<Map of Travel Agent 1's Location>>
<<Directions to get to Rental Car Company 1 from the standby facility>>

| Travel Agent 2 | |
|---|---|
| Address | |
| Phone Number | |

<<Map of Travel Agent 2's Location>>
<<Directions to get to Rental Car Company 1 from the standby facility>>

## Airports

| Airport 1 | |
|---|---|
| Address | |
| Phone Number | |

<<Map of Airport 1's Location>>
<<Directions to get to Rental Car Company 1 from the standby facility>>

| Airport 2 | |
|---|---|
| Address | |
| Phone Number | |

<<Map of Airport 2's Location>>
<<Directions to get to Rental Car Company 1 from the standby facility>>

## Operational Considerations

**Elective (Mandatory** where facilities exist**)**

If employees are required to stay at the Standby Facility for extended periods of time and require hotel accommodations, they will be provided by <<Organization Name>>. The Facilities Team will be responsible for determining which employees require hotel accommodations and ensuring sufficient rooms are made available.

If employees are required to stay at the Standby Facility for extended periods of time and require food, it will be provided by <<Organization Name>>. The Facilities Team will be responsible for determining which employees require food and ensuring sufficient is made available via groceries, restaurants or caterers as appropriate.

While in the Standby Facility, employees must work under appropriate, sanitary and safe conditions. The Facilities team will be responsible for ensuring that this facility is kept in proper working order.

Include only those operations considerations providers that are appropriate given the facilities of the Standby Facility.

## Accommodations

| | |
|---|---|
| **Hotel 1** | |
| **Address** | |
| **Phone Number** | |

<<Map of Hotel 1's Location>>
<<Directions to get to Hotel 1 from the standby facility>>

| | |
|---|---|
| **Hotel 2** | |
| **Address** | |
| **Phone Number** | |

<<Map of Hotel 1's Location>>
<<Directions to get to Hotel 2 from the standby facility>>

## Food, Beverages and Other Supplies

| | |
|---|---|
| **Restaurant/Grocery 1** | |
| **Address** | |
| **Phone Number** | |

<<Map of Restaurant/Grocery 1's Location>>
<<Directions to get to Restaurant/Grocery 1 from the standby facility>>

| **Restaurant/Grocery 2** | |
| --- | --- |
| **Address** | |
| **Phone Number** | |

<<Map of Restaurant/Grocery 2's Location>>
<<Directions to get to Restaurant/Grocery 2 from the standby facility>>

| **Restaurant/Grocery 3** | |
| --- | --- |
| **Address** | |
| **Phone Number** | |

<<Map of Restaurant/Grocery 3's Location>>
<<Directions to get to Restaurant/Grocery 3 from the standby facility>>

## Catering

| **Caterer 1** | |
| --- | --- |
| **Address** | |
| **Phone Number** | |

<<Map of Caterer 1's Location>>
<<Directions to get to Caterer 1 from the standby facility>>

| **Caterer 2** | |
| --- | --- |
| **Address** | |
| **Phone Number** | |

<<Map of Caterer 2's Location>>
<<Directions to get to Caterer 2 from the standby facility>>

## Standby Facility Maintenance

| **Maintenance Company** | |
| --- | --- |
| **Address** | |
| **Phone Number** | |

## Data and Backups

**Mandatory**

This section explains where all of the organization's data resides as well as where it is backed up to. Use this information to locate and restore data in the event of a disaster.

In this section it is important to explain where the organization's data resides. Discuss the location of all the organization's servers, backups and offsite backups and list what information is stored on each of these.

## Data in Order of Criticality

Please list all of the data in your organization in order of their criticality. Add or delete rows as needed to the table below.

| Rank | Data | Data Type | Back-up Frequency | Backup Location(s) |
|---|---|---|---|---|
| 1 | <<Data Name or Group>> | <<Confidential, Public, Personally identifying information>> | <<Frequency that data is backed up>> | <<Where data is backed up to>> |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |

# Communicating During a Disaster

**Mandatory**

In the event of a disaster <<Organization Name>> will need to communicate with various parties to inform them of the effects on the business, surrounding areas and timelines. The Communications Team will be responsible for contacting all of <<Organization Name>>'s stakeholders.

## Communicating with the Authorities

**Mandatory**

The Communications Team's first priority will be to ensure that the appropriate authorities have been notified of the disaster, providing the following information:

- Edit this list to reflect your organization
- *The location of the disaster*
- *The nature of the disaster*
- *The magnitude of the disaster*
- *The impact of the disaster*
- *Assistance required in overcoming the disaster*
- *Anticipated timelines*

## Authorities Contacts

Add or delete rows to reflect the media contacts your enterprise must contact.

| Authorities | Point of Contact | Phone Number | E-mail |
|---|---|---|---|
| *Police Department* | *<<Contact Name>>* | *111-222-3333* | *<<Contact E-mail>>* |
| *Fire Department* | *<<Contact Name>>* | *111-222-3333* | *<<Contact E-mail>>* |
|  |  |  |  |

## Communicating with Employees

### Mandatory

The Communications Team's second priority will be to ensure that the entire company has been notified of the disaster. The best and/or most practical means of contacting all of the employees will be used with preference on the following methods (in order):

- Edit this list to reflect your organization
- *E-mail (via corporate e-mail where that system still functions)*
- *E-mail (via non-corporate or personal e-mail)*
- *Telephone to employee home phone number*
- *Telephone to employee mobile phone number*

The employees will need to be informed of the following:

- Edit this list to reflect your organization
- *Whether it is safe for them to come into the office*
- *Where they should go if they cannot come into the office*
- *Which services are still available to them*
- *Work expectations of them during the disaster*

## Employee Contacts

Add or delete rows to reflect the employees in your organization.

| Name | Role/Title | Home Phone Number | Mobile Phone Number | Personal E-mail Address |
|---|---|---|---|---|
| *John Smith* | *Employee* | *111-222-3333* | *111-222-3333* | *jsmith@org.org* |
| *Fred Jones* | *Employee* | *111-222-3333* | *111-222-3333* | *fjones@org.org* |

## Communicating with Clients

### Mandatory

After all of the organization's employees have been informed of the disaster, the Communications Team will be responsible for informing clients of the disaster and the impact that it will have on the following:

- Edit this list to reflect your organization
- *Anticipated impact on service offerings*
- *Anticipated impact on delivery schedules*
- *Anticipated impact on security of client information*
- *Anticipated timelines*

Crucial clients will be made aware of the disaster situation first. Crucial clients will be E-mailed first then called after to ensure that the message has been delivered. All other clients will be contacted only after all crucial clients have been contacted.

## Crucial Clients

### Mandatory

Add or delete rows to reflect the crucial clients your enterprise must contact.

| Company Name | Point of Contact | Phone Number | E-mail |
|---|---|---|---|
| *<<Company Name>>* | *<<Contact Name>>* | *111-222-3333* | *<<Contact E-mail>>* |
| | | | |
| | | | |

## Secondary Clients

### Elective

Add or delete rows to reflect the secondary clients your enterprise must contact.

| Company Name | Point of Contact | Phone Number | E-mail |
|---|---|---|---|
| *<<Company Name>>* | *<<Contact Name>>* | *111-222-3333* | *<<Contact E-mail>>* |
| | | | |
| | | | |

## Communicating with Vendors

### Mandatory

After all of the organization's employees have been informed of the disaster, the Communications Team will be responsible for informing vendors of the disaster and the impact that it will have on the following:

- Edit this list to reflect your organization
- *Adjustments to service requirements*
- *Adjustments to delivery locations*
- *Adjustments to contact information*
- *Anticipated timelines*

Crucial vendors will be made aware of the disaster situation first. Crucial vendors will be E-mailed first then called after to ensure that the message has been delivered. All other vendors will be contacted only after all crucial vendors have been contacted.

Vendors encompass those organizations that provide everyday services to the enterprise, but also the hardware and software companies that supply the IT department. The Communications Team will act as a go-between between the DR Team leads and vendor contacts should additional IT infrastructure be required.

## Crucial Vendors

### Mandatory

Add or delete rows to reflect the crucial vendors your enterprise must contact.

| Company Name | Point of Contact | Phone Number | E-mail |
|---|---|---|---|
| *<<Company Name>>* | *<<Contact Name>>* | *111-222-3333* | *<<Contact E-mail>>* |
| | | | |
| | | | |

## Secondary Vendors

### Elective

Add or delete rows to reflect the secondary vendors your enterprise must contact.

| Company Name | Point of Contact | Phone Number | E-mail |
|---|---|---|---|
| *<<Company Name>>* | *<<Contact Name>>* | *111-222-3333* | *<<Contact E-mail>>* |
| | | | |
| | | | |

## Communicating with the Media
### Elective
After all of the organization's employees have been informed of the disaster, the Communications Team will be responsible for informing media outlets of the disaster, providing the following information:

- Edit this list to reflect your organization
- *An official statement regarding the disaster*
- *The magnitude of the disaster*
- *The impact of the disaster*
- *Anticipated timelines*

## Media Contacts
Add or delete rows to reflect the media contacts your enterprise must contact.

| Company Name | Point of Contact | Phone Number | E-mail |
|---|---|---|---|
| *<<Company Name>>* | *<<Contact Name>>* | *111-222-3333* | *<<Contact E-mail>>* |
| | | | |
| | | | |

## Communicating with <<Other group/stakeholders>>

### Elective
Specify additional contacts as required in your organization.

*Define the contact, the circumstances under which they are contacted, and the information that is communicated here.*

### Other Contacts
Add or delete rows to reflect the other contacts your enterprise must contact.

| Company Name | Point of Contact | Phone Number | E-mail |
|---|---|---|---|
| *<<Company Name>>* | *<<Contact Name>>* | *111-222-3333* | *<<Contact E-mail>>* |
| | | | |
| | | | |

# Dealing with a Disaster

## Mandatory

If a disaster occurs in <<Organization Name>>, the first priority is to ensure that all employees are safe and accounted for. After this, steps must be taken to mitigate any further damage to the facility and to reduce the impact of the disaster to the organization.

Regardless of the category that the disaster falls into, dealing with a disaster can be broken down into the following steps:

- Edit this list to reflect your organization
1) Disaster identification and declaration
2) DRP activation
3) Communicating the disaster
4) Assessment of current and and prevention of further damage
5) Standby facility activation
6) Establish IT operations
7) Repair and rebuilding of primary facility

# Disaster Identification and Declaration

## Mandatory

Since it is almost impossible to predict when and how a disaster might occur, <<Organization Name>> must be prepared to find out about disasters from a variety of possible avenues. These can include:

- Edit this list to reflect your organization
- *First hand observation*
- *System Alarms and Network Monitors*
- *Environmental and Security Alarms in the Primary Facility*
- *Security staff*
- *Facilities staff*
- *End users*
- *3rd Party Vendors*
- *Media reports*

Once the Disaster Recovery Lead has determined that a disaster had occurred, s/he must officially declare that the company is in an official state of disaster. It is during this phase that the Disaster Recovery Lead must ensure that anyone that was in the primary facility at the time of the disaster has been accounted for and evacuated to safety according to the company's Evacuation Policy.

While employees are being brought to safety, the Disaster Recovery Lead will instruct the Communications Team to begin contacting the Authorities and all employees not at the impacted facility that a disaster has occurred.

## DRP Activation

### Mandatory

Once the Disaster Recovery Lead has formally declared that a disaster has occurred s/he will initiate the activation of the DRP by triggering the Disaster Recovery Call Tree. The following information will be provided in the calls that the Disaster Recovery Lead makes and should be passed during subsequent calls:

- Edit this list as required
- *That a disaster has occurred*
- *The nature of the disaster (if known)*
- *The initial estimation of the magnitude of the disaster (if known)*
- *The initial estimation of the impact of the disaster (if known)*
- *The initial estimation of the expected duration of the disaster (if known)*
- *Actions that have been taken to this point*
- *Actions that are to be taken prior to the meeting of Disaster Recovery Team Leads*
- *Scheduled meeting place for the meeting of Disaster Recovery Team Leads*
- *Scheduled meeting time for the meeting of Disaster Recovery Team Leads*
- *Any other pertinent information*

If the Disaster Recovery Lead is unavailable to trigger the Disaster Recovery Call Tree, that responsibility shall fall to the Disaster Management Team Lead

## Communicating the Disaster

Refer to the "Communicating During a Disaster" section of this document.

## Assessment of Current and Prevention of Further Damage

### Mandatory

Before any employees from <<Organization Name>> can enter the primary facility after a disaster, appropriate authorities must first ensure that the premises are safe to enter.

The first team that will be allowed to examine the primary facilities once it has been deemed safe to do so will be the Facilities Team. Once the Facilities Team has completed an examination of the building and submitted its report to the Disaster Recovery Lead, the Disaster Management, Networks, Servers, and Operations Teams will be allowed to examine the building. All teams will be required to create an initial report on the damage and provide this to the Disaster Recovery Lead within <<state timeframe>> of the initial disaster.

During each team's review of their relevant areas, they must assess any areas where further damage can be prevented and take the necessary means to protect <<Organization Name>>'s assets. Any necessary repairs or preventative measures must be taken to protect the facilities; these costs must first be approved by the Disaster Recovery Team Lead.

## Standby Facility Activation
### Mandatory
The Standby Facility will be formally activated when the Disaster Recovery Lead determines that the nature of the disaster is such that the primary facility is no longer sufficiently functional or operational to sustain normal business operations.

Once this determination has been made, the Facilities Team will be commissioned to bring the Standby Facility to functional status after which the Disaster Recovery Lead will convene a meeting of the various Disaster Recovery Team Leads at the Standby Facility to assess next steps. These next steps will include:

- Edit this list to reflect your organization
1. Determination of impacted systems
2. Criticality ranking of impacted systems
3. Recovery measures required for high criticality systems
4. Assignment of responsibilities for high criticality systems
5. Schedule for recovery of high criticality systems
6. Recovery measures required for medium criticality systems
7. Assignment of responsibilities for medium criticality systems
8. Schedule for recovery of medium criticality systems
9. Recovery measures required for low criticality systems
10. Assignment of responsibilities for recovery of low criticality systems
11. Schedule for recovery of low criticality systems
12. Determination of facilities tasks outstanding/required at Standby Facility
13. Determination of operations tasks outstanding/required at Standby Facility
14. Determination of communications tasks outstanding/required at Standby Facility
15. Determination of facilities tasks outstanding/required at Primary Facility
16. Determination of other tasks outstanding/required at Primary Facility
17. Determination of further actions to be taken

During Standby Facility activation, the Facilities, Networks, Servers, Applications, and Operations teams will need to ensure that their responsibilities, as described in the "Disaster Recovery Teams and Responsibilities" section of this document are carried out quickly and efficiently so as not to negatively impact the other teams.

## Restoring IT Functionality
### Mandatory
Refer to the "Restoring IT Functionality" section of this document.

## Repair & Rebuilding of Primary Facility

### Elective

Before the enterprise can return operations to Primary Facilities, those facilities must be returned to an operable condition. The tasks required to achieve that will be variable depending on the magnitude and severity of the damage. Specific tasks will be determined and assigned only after the damage to Primary Facilities has been assessed.

## Other Organization Specific Steps Required

### Elective

Explain the steps to be taken

# Restoring IT Functionality

**Mandatory**

Should a disaster actually occur and <<Organization Name>> need to exercise this plan, this section will be referred to frequently as it will contain all of the information that describes the manner in which <<Organization Names>>'s information system will be recovered.

This section will contain all of the information needed for the organization to get back to its regular functionality after a disaster has occurred. It is important to include all Standard Operating Procedures documents, run-books, network diagrams, software format information etc. in this section.

## Current System Architecture

**Mandatory**

In this section, include a detailed system architecture diagram. Ensure that all of the organization's systems and their locations are clearly indicated.

<<System Architecture Diagram>>

## IT Systems

**Mandatory**

Please list all of the IT Systems in your organization in order of their criticality. Next, list each system's components that will need to be brought back online in the event of a disaster. Add or delete rows as needed to the table below.

| Rank | IT System | System Components (In order of importance) |
|------|-----------|--------------------------------------------|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |

## Criticality Rank-One System

In this section you will be required to rank each system's components in order of criticality, supplying the information that each system will require to bring it back online. First, vendor and model information, serial numbers and other component specific information will be gathered. Next, you will be required to attach each component's runbooks or Standard Operating Procedure (SOP) documents.

Each component must have a runbook or SOP document associated with it. If you do not have these documents for all components, please refer to the following Info-Tech Research Group notes for more information:

- SOP Research:
  o SOP 101: Standard Operating Procedures
  o How to Write an SOP
  o How to Implement SOPs
  o Step-by-Step SOP Template
  o Hierarchical SOP Template
  o Flowchart SOP Template
- Runbooks Research:
  o Don't Run without Runbooks
  o Free IT Staff Time: Implement Runbook Automation
  o How to Start Building Runbooks

*EXAMPLE:*

| System Name | <<State the name of the IT System here>> |
|---|---|
| Component Name | <<State the name of the specific IT Component here>> |
| Vendor Name | <<State the name of the IT Component's vendor here>> |
| Model Number | <<State the name of the IT Component's model number here>> |
| Serial Number | <<State the name of the IT Component's serial number here>> |
| Recovery Time Objective | <<State the IT Component's Recovery Time Objective here>> |
| Recovery Point Objective | <<State the IT Component's Recovery Point Objective here>> |

| | |
|---|---|
| **Title:** Standard Operating Procedures for <<Component Name>> | |
| **Document No.:** <<Number of the SOP document>> | |

| Security Level: << Public, Restricted, or Departmental (the specific department is named).>> | | Effective Date: <<The date from which the SOP is to be implemented and followed>> |
|---|---|---|
| SOP Author/Owner: | SOP Approver: | Review Date: <<The date on which the SOP must be submitted for review and revision>> |

### a) Purpose

This SOP outlines the steps required to restore operations of <<IT System Name>>.

### b) Scope

This SOP applies to the following components of <<IT System Name>>:

- Edit this list to include all included components of the system in question
- *Web server*
- *Web server software*
- *Application server*
- *Application server storage system*
- *Application server software*
- *Application server backup*
- *Database server*
- *Database server storage system*
- *Database server software*
- *Database server backup*
- *Client hardware*
- *Client software*

### c) Responsibilities

The following individuals are responsible for this SOP and for all aspects of the system to which this SOP pertains:

- Edit this list as required
- *SOP Process*: << SOP Owner>>
- *Network Connectivity*: <<Appropriate Network Administrator>>
- *Server Hardware*: <<Appropriate Systems Administrator>>
- *Server Software*: <<Appropriate Application Administrator>>
- *Client Connectivity*: <<Appropriate Network Administrator>>
- *Client Hardware*: <<Appropriate Helpdesk Administrator>>
- *Client Software*: <<Appropriate Helpdesk Administrator>>

For details of the actual tasks associated with these responsibilities, refer to section h) of this SOP.

**d) Definitions**

This section defines acronyms and words not in common use:

- Edit this list as required
- *Document No.*:  Number of the SOP document as defined by [insert numbering scheme]
- *Effective Date*:  The date from which the SOP is to be implemented and followed
- *Review Date*:  The date on which the SOP must be submitted for review and revision
- *Security Level*:  Levels of security are categorized as Public, Restricted, or Departmental
- *SOP*:  Standard Operating Procedure

**e) Changes Since Last Revision**

- Add to this list as required
- << Nature of change, date of change, individual making the change, individual authorizing the change>>

**f) Documents/Resources Needed for this SOP**

The following documents are required for this SOP:

- Add to this list as required
- *Document*

**g) Related Documents**

The following documents are related to this SOP and may be useful in the event of an emergency. Their documents below are hyperlinked to their original locations and copies are also attached in the appendix of this document:

- Add to this list as required
- *Document*

## h) Procedure

The following are the steps associated with bringing <<Component Name>> back online in the event of a disaster or system failure.

| Step | Action | Responsibility |
|------|--------|----------------|
| 1 | <<Step 1 Action>> | <<Person/group responsible>> |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |

## Criticality Rank-Two System

Repeat as above for as many systems as the enterprise makes use of.

# Plan Testing & Maintenance

## Mandatory

While efforts will be made initially to construct this DRP is as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the enterprise will change. As a result of these two factors this plan will need to be tested on a periodic basis to discover errors and omissions and will need to be maintained to address them.

For more information on DRP Testing and Maintenance, please refer to the following Info-Tech Research Group solution set for more information:

- [Make Sure the DRP is Ready for a Disaster](#)

## Maintenance

### Mandatory

The DRP will be updated <<indicate frequency>> or any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

- Edit this list as required
1. *Ensuring that call trees are up to date*
2. *Ensuring that all team lists are up to date*
3. *Reviewing the plan to ensure that all of the instructions are still relevant to the organization*
4. *Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals*
5. *Ensuring that the plan meets any requirements specified in new laws*
6. *Other organizational specific maintenance goals*

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the company, it is the responsibility of the Disaster Recovery Lead to appoint a new team member.

## Testing

### Mandatory

<<Organization Name>> is committed to ensuring that this DRP is functional. The DRP should be tested every <<indicate frequency>> in order to ensure that it is still effective. Testing the plan will be carried out as follows:

Select which method(s) your organization will employ to test the DRP

1) **Walkthroughs**- Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DRP project manager to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities (if required).

2) **Simulations**- A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. However, validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

3) **Parallel Testing**- A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.

4) **Full-Interruption Testing**- A full-interruption test activates the total DRP. The test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. The importance of due diligence with respect to previous DRP phases cannot be overstated.

Any gaps in the DRP that are discovered during the testing phase will be addressed by the Disaster Recovery Lead as well as any resources that he/she will require.

## Call Tree Testing
### Elective
Testing of the call trees is normally a good idea. Feel free to omit this section if you feel that it is irrelevant.

Call Trees are a major part of the DRP and <<Organization Name>> requires that it is tested every <<Enter time frame here>> in order to ensure that it is functional. Tests will be performed as follows:

1) Disaster Recovery Lead initiates call tree and gives the first round of employees called a code word.
2) The code word is passed from one caller to the next.
3) The next work day all Disaster Recovery Team members are asked for the code word.
4) Any issues with the call tree, contact information etc will then be addressed accordingly.

_____