**Questions:**

1. **What is business continuity plan? How it is different from Disaster recovery plan?**

Ans: **Business Continuity Plan (BCP) -**

A Business Continuity Plan or BCP is how an organization guards against future disasters that could endanger its long-term health or the accomplishment of its primary mission. BCPs take into account disasters that can occur on multiple geographic levels-local, regional, and national-disasters like fires, earthquakes, or pandemic illness. BCPs should be live and evolving strategies that are adjusted for any potential disasters that would require recovery; it should include everything from technological viruses to terrorist attacks. The ultimate goal is to help expedite the recovery of an organization's critical functions and manpower following these types of disasters. This sort of advanced planning can help an organization minimize the amount of loss and downtime it will sustain while simultaneously creating its best and fastest chance to recover after a disaster.

**Disaster Recovery Plan (DRP) -**

Disaster Recovery (DR) is the process an organization uses to recover access to their software, data, and/or hardware that are needed to resume the performance of normal, critical business functions after the event of either a natural disaster or a disaster caused by humans. While Disaster Recovery plans, or DRPs, often focus on bridging the gap where data, software, or hardware have been damaged or lost, one cannot forget the vital element of manpower that composes much of any organization. A building fire might predominantly affect vital data storage; whereas an epidemic illness is more likely to have an effect on staffing. Both types of disaster need to be considered when creating a DR Plan. Thus, organizations should include in their DRPs contingencies for how they will cope with the sudden and/or unexpected loss of key personnel as well as how to recover their data.

*Difference –*

BCP is all about how the Business continues to operate if something goes wrong. It is important to ensure that the ownership of this plan is with the business, as this drives the focus of the document. A properly defined BCP would include considerations such as paper processes, communication with customers and suppliers, staff relocation, location of other documents and contact details.

There should be a disaster recovery plan for IT, but there may be DR plans for other parts of the business too – such as manufacturing, customer interaction, logistics etc. – which in themselves would have disaster recovery plans for their own business capabilities and functions.

The big difference between BCP and DR plan is that a DRP will specify how the recovery of a function will be performed. Within a DR plan, there will be individual component system recovery plans that would specify steps to recover applications.

1. **Explain various components of DRP.**

Ans: Because your business involves several connected parts, a number of elements will go into a good disaster recovery strategy. It includes:

**1. Secure data storage -** If your network fails, the information it contains can be corrupted or lost. Preserving your data is essential to any plan to restore normal operations in good time.

**2. Regular backups -** A backup that was made weeks or months ago can force you to rebuild your most recent projects from scratch. Depending on how much data your business handles, even backing up your data on a daily basis might not be often enough.

**3. Quick detection -** Service interruptions can take many forms, and it’s important to know how exactly what the problem is in order to coordinate a response. Building in diagnostic tools to help you evaluate your system can be essential when coordinating your disaster recovery effort.

**4. Offsite locations -** Having a secondary site can help to keep your business running if your main office is damaged too badly to return to right away. Keeping offsite backups for your data will allow you to keep your company’s virtual presence running smoothly while you relocate to a new physical space.

**5. Service redundancy -** Even more than a physical location, it’s important to having a set of secondary resources, such as alternate communication lines to use if the phone network goes down, or backups for the company email server.

**6. Employee preparation -** Each of your employees must be familiar with the recovery plan, and what they need to do in the event of a disaster.

**7. Succession planning -** A great disaster recovery plan can fall apart if the particular employee it depends on is suddenly unavailable, and no one else knows how to step in. Your employees need backups, too.

**8. Awareness -** For many businesses, the weakest part of their disaster recovery plan is a lack of serious attention. Overcoming the human tendency to view a disaster as unlikely is critical to minimizing the damage if and when one occurs.

NMIMS Disaster Recovery Plan

Date

Version 1

Table of Contents

[Introduction 1](#_Toc273516726)

[Definition of a Disaster 1](#_Toc273516727)

[Purpose 1](#_Toc273516728)

[Scope 2](#_Toc273516729)

[Version Information & Changes 2](#_Toc273516730)

[Disaster Recovery Teams & Responsibilities 4](#_Toc273516731)

[Disaster Recovery Lead 5](#_Toc273516732)

[Disaster Management Team 6](#_Toc273516733)

[Network Team 8](#_Toc273516735)

[Server Team 9](#_Toc273516736)

[Disaster Recovery Call Tree 16](#_Toc273516743)

[Communicating During a Disaster 26](#_Toc273516749)

[Communicating with the Authorities 26](#_Toc273516750)

[Communicating with Employees 27](#_Toc273516751)

[Dealing with a Disaster 32](#_Toc273516756)

[Disaster Identification and Declaration 32](#_Toc273516757)

[DRP Activation 33](#_Toc273516758)

[Communicating the Disaster 33](#_Toc273516759)

[Assessment of Current and Prevention of Further Damage 33](#_Toc273516760)

[Restoring IT Functionality 36](#_Toc273516765)

[Current System Architecture 36](#_Toc273516766)

[IT Systems 36](#_Toc273516767)

# Introduction

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

## Definition of a Disaster

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

* *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:

* *Fire*
* *Flash flood*
* *Pandemic*
* *Power Outage*
* *Theft*
* *Terrorist Attack*

## Purpose

In the event of a disaster the first priority of NMIMS is to prevent the loss of life. Before any secondary measures are undertaken, NMIMS 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 NMIMS 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:

* *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

The NMIMS DRP takes all of the following areas into consideration:

* *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 NMIMS or contact Ash Ketchum at 12341234

## Version Information & Changes

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, NMIMS requires that the version number be updated to indicate this.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name of Person Making Change** | **Role of Person Making Change** | **Date of Change** | **Version Number** | **Notes** |
| *Ash Ketchum* | *DR Lead* | *01/01/09* | *1.0* | *Initial version of DR Plan* |

# Disaster Recovery Teams & Responsibilities

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 NMIMS. The different groups and their responsibilities are as follows:

* *Disaster Recovery Lead(s)*
* *Disaster Management Team*
* *Network Team*
* *Server Team*
* *Management Team*

The lists of roles and responsibilities in this section have been created by NMIMS 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.

## Disaster Recovery Lead

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 NMIMS, 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 NMIMS.

### Role and Responsibilities

* *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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role/Title** | **Work Phone Number** | **Home Phone Number** | **Mobile Phone Number** |
| *Ash Ketchum* | *Primary Disaster Lead* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Disaster Management Team

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.

### Role & Responsibilities

* *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 NMIMS*
* *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 NMIMS 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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role/Title** | **Work Phone Number** | **Home Phone Number** | **Mobile Phone Number** |
| *Ash Ketchum* | *Primary disaster lead* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Network Team

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

* *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:*
  + *All members of the DR Teams*
  + *All C-level and Executive Staff*
  + *All IT employees*
  + *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 NMIMS 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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role/Title** | **Work Phone Number** | **Home Phone Number** | **Mobile Phone Number** |
| *Ash Ketchum* | *Network Manager* | *111-222-3333* | *111-222-3333* | *111-222-3333* |

## Server Team

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

* *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:*
  + *Assess the damage to any servers*
  + *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 NMIMS’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 NMIMS 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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role/Title** | **Work Phone Number** | **Home Phone Number** | **Mobile Phone Number** |
| *Ash Ketchum* | *Operations Manager* | *111222-3333* | *111-222-3333* | *111-222-3333* |

# Disaster Recovery Call Tree

In a disaster recovery or business continuity emergency, time is of the essence so NMIMS 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  *Ash Ketchum* | | | *111-222-3333* | *111-222-3333* | *111-222-3333* |
|  | DR Management Team Lead  Misty | | 222-333-444 | 222-333-444 | 222-333-444 |
|  | | DR Management Team 1  Brock | 333-444-555 | 333-444-555 | 333-444-555 |
|  | | DR Management Team 2  Draco | 444-555-666 | 444-555-666 | 444-555-666 |
|  | Facilities Team Lead  Jenny | | 555-666-777 | 555-666-777 | 555-666-777 |
|  | | Facilities Team 1  Malfoy | 666-777-888 | 666-777-888 | 666-777-888 |



# Communicating During a Disaster

In the event of a disaster NMIMS 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 NMIMS‘s stakeholders.

## Communicating with the Authorities

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

* *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

|  |  |  |  |
| --- | --- | --- | --- |
| **Authorities** | **Point of Contact** | **Phone Number** | **E-mail** |
| *Police Department* | *Off. Jenny* | *100* | *offjenni@fastmail.fm* |
| *Fire Department* | *Squirtle Squirtle* | *101* | *squirt@gmail.com* |

## Communicating with Employees

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):

* *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:

* *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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role/Title** | **Home Phone Number** | **Mobile Phone Number** | **Personal E-mail Address** |
| *Ash Ketchum* | *Employee* | *111-222-3333* | *111-222-3333* | *jsmith@org.org* |

# Dealing with a Disaster

If a disaster occurs in NMIMS, 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:

1. Disaster identification and declaration
2. DRP activation
3. Communicating the disaster
4. Assessment of current and prevention of further damage

## Disaster Identification and Declaration

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

* *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

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:

* *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

Before any employees from NMIMS 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 two weeks 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 NMIMS’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.

# Restoring IT Functionality

Should a disaster actually occur and NMIMS 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 NMIMS’s information system will be recovered.

## Current System Architecture

## IT Systems

|  |  |  |
| --- | --- | --- |
| **Rank** | **IT System** | **System Components (In order of importance)** |
| 1 | SAP Database |  |
| 2 | NMIMS Network |  |
| 3 | Server Room Control |  |
| 4 | Faculty Access |  |
| 5 | Student Access |  |