A picture containing text, graphics, font, graphic design

Description automatically generated

**Disaster Recovery Plan V2.0**

**To Ensure Business Continuity (BCP)**

02-Aug-2023

A black background with blue text

Description automatically generated

**Document Owner:**

Vijayakumar N

System Administrator data center

Piramal foundation

9154622513

vijay.nuthalpati@piramalswasthya.org

Table of Contents

[Introduction 2](#_Toc428521535)

[Definition of a Disaster 2](#_Toc428521536)

[Purpose 2](#_Toc428521537)

[Scope 2](#_Toc428521538)

[Version Information & Changes 3](#_Toc428521539)

[Disaster Recovery Teams & Responsibilities 4](#_Toc428521540)

[Disaster Management Team 4](#_Toc428521541)

[Network Team 5](#_Toc428521542)

[Server Team 5](#_Toc428521543)

[Applications Team 6](#_Toc428521544)

[DataBase Team 6](#_Toc428521544)

[Senior Management Team 7](#_Toc428521545)

[Other Organization Specific Teams 7](#_Toc428521546)

[Disaster Recovery Call Tree 9](#_Toc428521547)

[Recovery Facilities 12](#_Toc428521548)

[Description of Recovery Facilities 12](#_Toc428521549)

[Transportation to the Standby Facility 14](#_Toc428521550)

[Data and Backups 14](#_Toc428521551)

[Communicating During a Disaster 16](#_Toc428521552)

[Communicating with Employees 16](#_Toc428521553)

[Communicating with Clients 16](#_Toc428521554)

[Communicating with Vendors 17](#_Toc428521555)

[Communicating with <<Other group/stakeholders>> 17](#_Toc428521556)

[Activating the Disaster Recovery Plan 18](#_Toc428521557)

[DRP Activation 18](#_Toc428521558)

[Assessment of Current and Prevention of Further Damage 18](#_Toc428521559)

[Standby Facility Activation 19](#_Toc428521560)

[Restoring IT Functionality 19](#_Toc428521561)

[Current System Architecture 20](#_Toc428521562)

[IT Systems 20](#_Toc428521563)

[Plan Testing & Maintenance 24](#_Toc428521564)

[Maintenance 24](#_Toc428521565)

[Testing 24](#_Toc428521566)

[Call Tree Testing 25](#_Toc428521567)

# Introduction

This Disaster Recovery Plan (DRP) captures, in a single repository, all of the information that describes Piramal Foundation’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 Piramal Foundation not being able to perform all or some of their regular roles and responsibilities for a period of time. Piramal Foundation defines disasters as the following:

* *One or more vital Server systems are non-functional.*
* *The Data Center is available, but all Server systems are non-functional.*
* *The Data Center building infra/Network is not available for an extended period, but all systems are functional within it.*
* *The Data Center 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*
* *Power Outage*
* *Theft*
* *Ransomware/Virus Pandemic*
* *Pandemic*
* *Earthquake*
* *War*
* *Terrorist Attack*

## Purpose

*Note that in the event of a disaster the first priority of Piramal Foundation is to prevent the loss of life. Before any secondary measures are undertaken, we will ensure that all employees and any individuals on the organization’s premises, are safe and secure.*

After all individuals are deemed safe, the next goal will be to follow the steps in this DRP to restore services 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 Piramal Foundation 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*

## Projects Deployed in Hyderabad Piramal Swasthya Facility DC

Piramal Foundation has multiple projects in PAN India and are deployed in Multiple states in their respective Data centers, in this document we will concentrate on Project which are Deployed in Hyderabad Data center under Piramal swasthya Office, which are mentioned below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name of Project/Server** | **URL** | **Local Server IP** | **OS & DB** | **Stack** |
| *NACO 1097 CC* | *http://192.168.35.218:8080/1097ui-v1.0/#/loin* | *192.168.35.218* | *Windows/ MySql* | *AMRIT* |
| *NACO GR* | *http://grievance1097naco.piramalswasthya.org/* | *192.168.35.150* | *Ubunut/ MySql* | *GR* |
| *C-Zentrix CTI* | *http://192.168.35.239/* | *192.168.35.239* | *Windows/ MySql* | *AMRIT* |
| *Sehat OK (Sanofi) TM, MMU* | [*https://amritmh.piramalswasthya.org/tmui-v1.0/#/login*](https://amritmh.piramalswasthya.org/tmui-v1.0/#/login)  [*https://amritmh.piramalswasthya.org/mmuui-v1.0/#/login*](https://amritmh.piramalswasthya.org/mmuui-v1.0/#/login) | *192.168.45.73* | *Windows/ MySql* | *AMRIT* |
| *STFC, MMU* | *https://stfc.piramalswasthya.org/mmuui-v1.0/#/login* | *192.168.45.178* | *Windows/ MySql* | *AMRIT* |
| *Bayer, TM, MMU* | [*https://bayertmc.piramalswasthya.org/tmui-v1.0/#/login*](https://bayertmc.piramalswasthya.org/tmui-v1.0/#/login)  *https://bayertmc.piramalswasthya.org/mmuui-v1.0/* | *192.168.45.74* | *Windows/ MySql* | *AMRIT* |
| *Digwall TM* | *https://amritap.piramalswasthya.org/tmui-v1.0/#/login* | *192.168.45.109* | *Windows/ MySql* | *AMRIT* |
| *APL TM* | [*https://apl.piramalswasthya.org/tmui-v1.0/#/login*](https://apl.piramalswasthya.org/tmui-v1.0/#/login) | *192.168.45.166* | *Windows/ MySql* | *AMRIT* |
| *BPSL-BSL Jharkand* | *https://175.101.1.226/* | *192.168.45.131* | *Windows/ MySql* | *AMRIT* |
| *SWYMED APP* | *http://psmri.swymed.com/* | *192.168.45.132* | *Windows/ SQL 2014* | *SWYMED* |

## 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, Piramal Foundation 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** |
| *Saleem Syed* | *DR Lead* | *01/01/20* | *1.0* | *Initial version of DR Plan* |
| *Vijay Kumar N* | *System Admin* | *08/02/23* | *2.0* | *Revised to include new Backup solution* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 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 Piramal Foundation. The different groups and their responsibilities are as follows:

* *Disaster Management Team*
* *Network Team*
* *Server Team*
* *Applications Team*
* *Database Team*
* *Senior Management Team*
* *Administrative Team*

## 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.

This will be the team responsible for all communication during a disaster. Specifically, they will communicate with **Piramal Foundation** employees, Stake holders, clients, vendors and suppliers, banks, and even the media if required.

### 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 Piramal Foundation*
* *Verify all backup and try to restore servers from the historical backups.*
* *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 Stake holders and relevant parties once the disaster is over and normal business functionality has been restored*
* *After Piramal Foundation 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** |
| *Saleem Syed* | *Primary Disaster Lead* | *9502811577* |  | *8919289198* |
| *Ramana Vadapalli* | *Secondary Disaster Lead* | *8008855563* |  | *8688039540* |
| *Vijay Kumar N* | *Tertiary Disaster Lead* | *9154622513* |  | *8867987969* |

## 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 s 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-Band and Executive Staff*
  + *All IT employees*
  + *All remaining employees*
* *Provide Connectivity for Backup solution Server so that server can be recovered from Cloud or NAS storage.*
* *Install and implement any tools, hardware, software and systems required in the standby facility in Assam*
* *Install and implement any tools, hardware, software and systems required in the primary facility in Hyd*
* *After Piramal Foundation is back to business as usual, this team will be summarizing 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** |
| *Surya Ramana* | *Network Administrator* | *9515264766* |  |  |
| *Nageshwar Rao* | *Network Vendor* |  |  |  |

## 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*
  + *Activate Replication server as primary in case there are replications.*
  + *Restore server data for Backup copies created in Backup server*
* *Ensure that Server can be restored with Backups taken form Veeam backup solution in primary location.*
* *Try to restore Few servers using Archive backup take using Veeam Backup solution in primary location*
* *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 Piramal Foundation 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 Piramal Foundation 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** |
| *Vijayakumar N* | *Systems Administrator* |  |  |  |
| *Sachin Kadam* | *Systems Administrator* |  |  |  |
|  |  |  |  |  |

## Applications Team

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

* *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:*
  + *Assess the impact to application processes*
  + *Restart applications as required*
  + *Patch, recode or rewrite applications as required*
* *Try to restore Required Application using backup copy taken from Backup Solution.*
* *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 Piramal Foundation 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** |
| *Intikhab Allam* | *Program Manager* |  |  |  |
| *Shashank K* | *Product Manager* |  |  |  |
| *Bala Murgan* | *Manager L2* |  |  |  |
| *Avinash Sharma* | *L2 Admin* |  |  |  |
| *Pavan G WIPRO* | *Application Manager* |  |  |  |

## Database Team

The Database Team will be responsible for ensuring that all enterprise Database restoration 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 database are restored to correct application 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 applications Database are not functioning at the primary facility*
* *If multiple applications Databases are impacted, the team will prioritize the recovery of applications Databases in the manner and order that has the least business impact. Recovery will include the following tasks:*
  + *Assess the impact to application Databases*
  + *Restore applications Databases as required*
  + *Patch, recode or rewrite applications Databases as required*
* *Try to restore Required Application Databases using backup copy taken from Backup Solution*
* *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 Piramal Foundation DC 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** |
| *Atul Goyal* | *Database Manager* |  |  |  |
| *Anil Mokirala WIPRO* | *Database Manager* |  |  |  |

## Senior Management Team

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 made by the Senior Management Team. The Disaster Recovery Lead will ultimately report to this team.

### Role & Responsibilities

* *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:*
  + *Rebuilding of the primary facilities*
  + *Rebuilding of data centers*
  + *Significant hardware and software investments and upgrades*
  + *Other financial and business decisions*

### Contact Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role/Title** | **Work Phone Number** | **Home Phone Number** | **Mobile Phone Number** |
| *Dhaivat Anjaria* | *CEO* |  |  |  |
| *Nithin Rathanam* | *COO* |  |  |  |
| *Raja Sekhar Kalki* | *CTO* |  |  |  |

## Administrative Team

The Administrative Team will assist DR team in relocation, Purchasing, coordination with Vendors and Transportation, if in case. Decisions such as constructing a new data center, relocating the primary site etc. All this activity should be carried out by or in observation of the Administrative Team. The Disaster Recovery Lead will take support of this team.

### Role & Responsibilities

* *Ensure that the Disaster Recovery Team Lead is getting all the support required.*
* *Coordinate with Vendors on AMC and new procurement*
* *Assist in Transportation and addressing safety of employees, Documentation and Equipment’s .*
* *Assist Data center team and infra team on getting things restored in timely manner.*
* *Asist in decisions making concerning:*
  + *Rebuilding of the primary facilities*
  + *Rebuilding of data centers*
  + *Significant hardware and software investments and upgrades*
  + *Other financial and business decisions*

### Contact Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role/Title** | **Work Phone Number** | **Home Phone Number** | **Mobile Phone Number** |
| *GNK Reddy* | *Procurement Manager* |  |  |  |
| *Vadi Raj* | *Procurement Lead* |  |  |  |
| *Rajani Ravindran* | *Administrative Manager* |  |  |  |

# Disaster Recovery Call Tree

In a disaster recovery or business continuity emergency, time is of the essence so Piramal Foundation 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).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Contact** | | | | | **Office** | **Mobile** | **Home** |
| DR Lead  *Saleem Syed* | | | | |  |  |  |
|  | DR Management Team Lead  Ramana V | | | |  |  |  |
|  | | | | DR Management Team 1  Vijay Kumar N |  |  |  |
|  | | | | DR Management Team 2 |  |  |  |
|  | Facilities Team Lead  GNK Reddy | | | |  |  |  |
|  | | | | Facilities Team 1  Rajani |  |  |  |
|  | Network Team Lead  Surya Ramana | | | |  |  |  |
|  | | LAN Team 1  Krishna Kiran Yadav | | |  |  |  |
|  | | | LAN Team 2 | |  |  |  |
|  | | WAN Team Lead Secondary location.  Hitesh T | | |  |  |  |
|  | | | WAN Team 1 | |  |  |  |
|  | Server Team Lead  Vijay Kumar N | | | |  |  |  |
|  | | Server Type 1  Sachin kadam | | |  |  |  |
|  | Applications Team Lead  Shashank K | | | |  |  |  |
|  | | App 1 Team Lead  Madhav | | |  |  |  |
|  | | | App1 Team 1  Varinder | |  |  |  |
|  | | App 2 Team Lead  Bala Murgan | | |  |  |  |
|  | | | App 2 Team 1  Avinash Sarma | |  |  |  |
|  | Management Team Lead  Raja Sekhar Kalki | | | |  |  |  |
|  | | | | Management Team 1  Ishmeet Singh |  |  |  |
|  | | | | Management Team 2  Intekhab A |  |  |  |
|  | Operations Team Lead  Nithin Rathnam | | | |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | Operations Team 1  Madhu Telugu |  |  |  |
|  | Finance Team Lead  Dharama Raj B | |  |  |  |
|  | | Finance Team 1  Srinivas |  |  |  |

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.



# Recovery Facilities

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

## Description of Recovery Facilities

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

Primary Data center Facility:

**Piramal Swasthya Management and Research Institute**

       3rd. Floor, Awfis, Oyster Complex, Somajiguda,

       Begumpet, Hyderabad - 500016. India

Standby Facility DRS site:

is 2,366.4 km away from the primary facility.

**Piramal Swasthya Management and Research Institute**

**G Sharma Baruah Building, Bamunimaidam,**

**Guwahati-781021, Assam. India**

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 Piramal Foundation, Piramal Swasthya.

The standby facility must always have the following resources available:

* *Copies of this DRP document*
* *Fully redundant server room or Data center*
* *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

***Assam Facility Map***

A map of a city

Description automatically generated

### Directions to Recovery Facility

### Standby Facility Maintenance

|  |  |
| --- | --- |
| **Maintenance Company** | Piramal Foundation ( AKA Piramal Swasthya Management and Research Institute ) |
| **Address** | G Sharma Baruah Building, Bamunimaidam,  Guwahati-781021, Assam. India |
| **Phone Number** | 9957557548, 8011417104 |

## Transportation to the Standby Facility

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 2,366.4 km 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.

### Flight Providers

|  |  |
| --- | --- |
| **Flight Company 1** |  |
| **Address** |  |
| **Phone Number** |  |

### Taxi Providers

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

|  |  |
| --- | --- |
| **Taxi Company 2** |  |
| **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.

### Data in Order of Criticality

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rank** | **Data** | **Data Type** | **Back-up Frequency** | **Backup Primary Location(s)** | **Backup Secondary Location(s)** |
| 1 | Production Server | Confidential | Daily | NAS, EHDD, Hardened Linux Server | Assam DC & Cloud AWS S3 |
| 2 | Development Servers | Confidential | Monthly | NAS, EHDD, Hardened Linux Server | Cloud AWS S3 |
| 3 | Non-Production | Informational | Monthly | NAS, EHDD, Hardened Linux Server |  |
| 4 | Testing Server | Informational | Quarterly Archive Backup | NAS, EHDD |  |
| 5 | Support Servers | Informational | Quarterly Archive Backup | NAS, EHDD |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |

# Communicating During a Disaster

In the event of a disaster, Piramal Foundation 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 Piramal Foundation’s stakeholders.**

## 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** |
| *Monica L* | *Admin* |  |  |  |
| *Reshma Pilley* | *Team Lead NACO* |  |  |  |
| *Krishna Kiran Yadav* | *IT Executive* |  |  |  |
| *Vijay Kumar J* | *Desktop Admin* |  |  |  |
| *Aravind Swasmy* | *IT Engineer* |  |  |  |
| *Naresh D* | *Finance* |  |  |  |
| *Rajendra* | *Office staff* |  |  |  |
| *Srinivas Rao* | *Finance* |  |  |  |
| *Mahender* | *Office staff* |  |  |  |

## Communicating with Clients

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:

* *Anticipated impact on service offerings*
* *Anticipated impact on delivery schedules*
* *Anticipated impact on security of client information*
* *Anticipated timelines*
* *Anticipated delay in response*

## Communicating with Vendors

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:

* *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 Called and then E-mailed 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.

|  |  |  |  |
| --- | --- | --- | --- |
| **Company Name** | **Point of Contact** | **Phone Number** | **E-mail** |
| Kamal Veer | PGK MURTHY | 8886331774 |  |
| CLOUDACE TECHNOLOGIES PRIVATE LIMITED | **Nageshwar Rao P** | M: +919959590088 | 040-40000338 | nageshwar@cloudace.in |
| **Veeam Backup** | **Debashish Roy** | **8904567728** |  |

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

*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>>* |
|  |  |  |  |
|  |  |  |  |

# Activating the Disaster Recovery Plan

If a disaster occurs in Piramal Foundation 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
5. Standby facility activation
6. Establish IT operations
7. Repair and rebuilding of primary facility
8. Raise complaint file legal suit in case Theft .

## 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*
* *Post information to all stake holders.*
* *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

## Assessment of Current and Prevention of Further Damage

Before any employees from Piramal Foundation 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 Piramal Foundation 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 Piramal Foundation 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

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:

1. *Determination of impacted systems*
2. *Criticality ranking of impacted systems*
3. *Recovery measures required for high criticality Production Server and Network systems*
4. *Assignment of responsibilities for high criticality Production Server and Network systems*
5. *Schedule for recovery of high criticality Production Server and Network systems*
6. *Recovery measures required for medium criticality Dev and Non-prod systems*
7. *Assignment of responsibilities for medium criticality Dev and Non-prod systems*
8. *Schedule for recovery of medium criticality Dev and Non-prod systems*
9. *Recovery measures required for low criticality Testing systems*
10. *Assignment of responsibilities for recovery of low Testing criticality systems*
11. *Schedule for recovery of low criticality Testing 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

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

## Current System Architecture

**Data Center System Architecture Diagram (temporary diagram only)**

A diagram of a computer network

Description automatically generated

**Production Server Architecture Diagram (temporary diagram only)**

A diagram of a computer network

Description automatically generated

**Backup Solution Architecture Diagram**

A diagram of a network

Description automatically generated

## IT Systems

|  |  |  |
| --- | --- | --- |
| **Rank** | **IT System** | **System Components (In order of importance)** |
| 1 | Physical Host Server |  |
| 2 | Network Devices |  |
| 3 | Production Servers |  |
| 4 | Storage Servers and devices |  |
| 5 | Communication devices |  |
| 6 | Monitoring Devices |  |
| 7 | Temperature devices |  |
| 8 | UPS and Power source |  |
| 9 |  |  |

Physical Server list:

|  |  |  |  |
| --- | --- | --- | --- |
| **SN** | **Make** | **SN** | **Host/ Client Operating system** |
| 1 | DELL Power Edge R-430 | 8167NK2 | Windows 2016 DC |
| 2 | DELL Power Edge R-430 | 8119NK2 | Windows 2016 DC |
| 3 | DELL Power Edge R-430 | 8116NK2 | Windows 2016 STD |
| 4 | DELL Power Edge R-430 | 8117NK2 | Windows 2016 STD |
| 5 | DELL Power Edge R-430 | 8179NK2 | Czentrix-UAT |
| 6 | DELL Power Edge R-430 | 8118NK2 | Windows 2016 DC |
| 7 | DELL Power Edge R-430 | 8196NK2 | Windows 2016 DC |
| 8 | DELL Power Edge R-430 | 818CNK2 | Windows 2016 DC |
| 9 | DELL Power Edge R-430 | 8187NK2 | Windows 2016 Std |
| 10 | DELL Power Edge R-430 | 819CNK2 | VM-ESXI-6 |
| 11 | Tyron Supermicro X9DRH-7TF | C825OFD44N10400 | VM-ESXI-6 |
| 12 | Tyron Supermicro X9DRH-7TF | C825OFD44N10445 | VM-ESXI-6 |
| 13 | Tyron Supermicro X9DRH-7TF | C825OFD24MB0332 | VM-ESXI-6 |
| 14 | Tyron Supermicro X9DRH-7TF | C825OFD24MB0334 | Windows 2016 DC |
| 15 | Dell EMC R540 | CRB28Q2 | VM-ESXI-6 |
| 16 | Dell EMC R540 | GQV525S2 | Ubunut 20Lts |
| 17 | Dell EMC R540 | J4HD823 | VM-ESXI-6 |
| 18 | Dell EMC R540 | CRC28Q2 | VM-ESXI-6 |
| 19 | Dell EMC R540 | GQT42S2 | VM-ESXI-6 |
| 20 | HP Proliant DL380 | SGH850T7NP | Windows 2016 Std |
| 21 | HP Proliant DL380 | SGH850T7NW | Windows 2016 STD |
| 22 | Tyron Supermicro X9DRH-7TF | 2X22481902 | Windows 2016 STD |
| 23 | Tyron Supermicro X9DRH-7TF | 2X22471902 | Windows 2016 Std |
| 24 | Tyron Supermicro X9DRH-7TF | 2X20621805 | VM-ESXI-6 |
| 25 | Tyron Supermicro X9DRH-7TF | 2X20631805 | Windows 2016 STD |
| 26 | DELL Power Edge 2950 | 5BYJT18 | Windows 2016 STD |
| 27 | DELL Power Edge 2950 | 5BYJT1S | Windows 2016 STD |
| 28 | Tyron Supermicro X9DRH-7TF | C8280FC37M80035 | VM-ESXI 6.0.3-5572656-NEC-6.0.3 |
| 29 | Tyron Supermicro X9DRH-7TF | C8250FE44N30588 | Centos 8 |
| 30 | Tyron Supermicro X9DRH-7TF | C8250FD47N11277 | Windows 2016 STD |
| 31 | HP Proliant DL60 | SGH616WWAL | OFF |
| 32 | Tyron Supermicro X9DRH-7TF | C8280FC37M80335 | Windows 2016 STD |
| 33 | HP Proliant DL380 | SGH616WWBB | Windows 2016 STD |
| 34 | HP Proliant DL380 | SGH616WWAY | Windows 2016 STD |
| 35 | HP Proliant DL380 | SGH616WWAL | Windows 2016 STD |
| 36 | HP Proliant DL380 | SGH616WWAL | Windows 2016 STD |
| 37 | IBM-SYSTEM X 3650 M4 | 06VAKK9 | VM-ESXI-6 |
| 38 | Lenovo ThinkSystem SR550 | J3005MH9 | Windows 2016 DC |
| 39 | ThinkSystem SR650 | J303GK61 | Windows 2016 DC |
| 40 | ThinkSystem SR650 | J3010CL5 | Windows 2016 STD |
| 41 | IBM X3630M4 | 06CEBXW | OFF |
| 42 | Tyron Supermicro X9DRH-7TF | C82S0FE44N30581 | Windows 2016 DC |
| 43 | Lenovo Think System SR650 | J30A7PLP | Windows 2016 DC |
| 44 | Lenovo Think System SR550 | J9008VXR | Windows 2016 STD |
| 45 | Lenovo Think System SR550 | J9008VXT | Windows 2016 STD |
| 46 | Lenovo Think System SR550 | J9008VXN | Windows 2016 STD |
| 47 | Lenovo Think System SR650 | J900AAEB | Windows 2016 DC |

**Production VM List:**

**Network Devices List:**

### Criticality Priority 1 System

**SOP :**

1. SOP 101: Standard Operating Procedures
2. SOP for Restoring Physical server
3. SOP for restoring VM
4. SOP to restore Host Hyper Server
5. SOP to installation of Applications in Server

**Runbooks Research:**

Don't Run without 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>> |

1. **Purpose**

This SOP outlines the steps required to restore operations of Production Servers.

1. **Scope**

This SOP applies to the following components of Production Server Application and Database:

* *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*

1. **Responsibilities**

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

* *SOP Process*: Vijay Kumar N
* *Network Connectivity*: Surya Ramana
* *Server Hardware*: Sachin Kadam
* *Server Software*: Avinash Sharma
* *Database package:* Atul Goyal
* *Client Connectivity*: Help Desk IT
* *Client Hardware*: Help Desk IT
* *Client Software*: Help Desk IT

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

1. **Definitions**

This section defines acronyms and words not in common use:

* *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

1. **Changes Since Last Revision**

* Added Backup Solution Infra, Veeam Backup solution is procured for Enterprises.

1. **Documents/Resources Needed for this SOP**

The following documents are required for this SOP:

* *Document*

1. **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:

* *Document*
* *SOP 101: Standard Operating Procedures*
* *SOP for Restoring Physical server*
* *SOP for restoring VM*
* *SOP to restore Host Hyper Server*
* *SOP to installation of Applications in Server*

1. **Procedure**

The following are the steps associated with bringing EXIC Host Servers 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 |  |  |

The following are the steps associated with bringing Windows Hyper -V Host Servers 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 |  |  |

The following are the steps associated with bringing Production Servers 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 Priority 2 System

The following are the steps associated with bringing Network Firewall 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 |  |  |

The following are the steps associated with bringing network Switches 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 |  |  |

The following are the steps associated with bringing Storage Server and Devices 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 |  |  |

# Plan Testing & Maintenance

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.

## Maintenance

The DRP will be updated Quarterly 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:

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

Piramal Foundation is committed to ensuring that this DRP is functional. The DRP should be tested every 6 months /Half yearly in order to ensure that it is still effective. Testing the plan will be carried out as follows:

**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).

1. **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.
2. **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.
3. **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.

## DR Team Call Tree Testing

Call Trees are a major part of the DRP and Piramal foundation requires that it is tested every 6 months/half yearly 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.

**Credits:**

**Digital Bharat Collaborative Team**