DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

By
IT Department
Repco Home Finance Limited
Version 6.0

TABLE OF CONTENTS

Contents

1. Introduction

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

A DISASTER is defined as an interruption of mission critical information services for an unacceptable period of time. An interruption of business during the company's working hours may create greater problem than that occurs after the business hours. Similarly, the period of interruption defines its characterization as a disaster – major or minor. Identification of major or minor disasters has a direct link to the anticipated time required for restoration to normalcy in the operation and retrieval of entire data / information from the system without any loss.

A DRP is a plan that defines the activities to be performed to bring back the business operations back to normal, in the event of and during a disaster.

Disaster Recovery Plan (DRP) is generally intended to identify and assess the events that pose a threat to business continuity, to determine the likely consequences and costs for deciding which business activities prioritizes for recovery and to draw procedures for speedy recovery from disaster. The plan should accomplish three objectives to:

- Manage an immediate crisis.
- Initiate actions to enable the business to continue in the short term.
- Establish the organizational procedure to manage medium and long-term recovery.

Disaster Recovery Planning aims at minimizing loss potentials through the development of capabilities and procedures in the wake of non-speculative interruptions of critical business functions.

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

- Fire
- Flood
- Power Outage
- War
- Theft
- Terrorist Attack
- Hardware Failure
- Earthquake
- Any other natural calamity
- Bandh, Civil unrest etc

DISASTER EVENTS:

Outage of Services and not recoverable for next 8 hours or above which may happen of the following events:

- Hard disk crash resulting in loss of critical data.
- Virus attacks resulting in loss of critical data/stoppage of critical applications.
- Hacking of core banking application resulting in misuse of important data.
- Network attacks resulting in unauthorized access to confidential data.
- Hardware theft resulting in monetary loss.
- Fire resulting in loss of software, data, and hardware.
- Electricity failure because of natural calamities, like storm, heavy rain, flood, grid problem at service provider side resulting in hard disk failure, data corruption, application instability.
- Human error such as an administrator accidentally erasing data or crashing a network.
- Network failure & not recoverable for next 8 hours or above.

2. Purpose and Scope

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

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

After all individuals have been brought to safety, the next goal of RHFL is 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.

Scope

The RHFL's DRP takes all of the following areas into consideration,

- Network Infrastructure
- Server Infrastructure
- Data Storage and Backup Systems
- End-user Computers
- Application Software Systems
- Database Systems
- IT Documentation

3. Version Information & Changes

Any changes, edits and updates made to the DRP are to 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, RHFL requires that the version number be updated to indicate this.

Date	Document Version	Document Revision History	Document Author
08.02.2016	1.0	Initial Document	Sri. M.Kangasabai (AGM-IT)
21.03.2016	1.0	First Review	Sri. K.Pandiarajan (AGM –IT)
08.05.2018	2.0	Second Review	Sri. K.Pandiarajan (AGM –IT)
13-05-2022	3.0	Third Review	Sri. K.Pandiarajan (GM –IT)
26-04-2024	4.0	Fourth Review	Sri. K.Pandiarajan (GM –IT)
11-07-2024	5.0	Fifth Review	Sri. K.Pandiarajan (GM –IT)
20-12-2025	6.0	6th Review	Sri. K.Pandiarajan (GM –IT)

Approvals

Date	Document Version	Approver Name and Title	Approver Signature
18.04.2016	**1.0**	**Sri. V. Raghu, Executive Director**	
09.05.2018	**2.0**	**Sri. Arun Kumar Mishra, Chief Development Officer**	
13.05.2022	**3.0**	**Sri. Bala Subramanian, Chief Development Officer**	
26-04-2024	**4.0**	**Sri. Vaidyanathan, Chief Development Officer**	
11-07-2024	**5.0**	**Sri. Vaidyanathan, Chief Development Officer**	
20-12-2025	**6.0**	**Sri. Vaidyanathan, Chief Development Officer**	

4. Disaster Recovery Teams & Responsibilities

In the event of a disaster, different groups are required to assist IT and Administration department in their effort to restore normal functionality to the staff members of RHFL. The different groups and their responsibilities are as follows:

- Disaster Recovery Lead(s)
- Disaster Management Team
- Administration Department Team
- Network Team
- Server Team
- Applications Team

The lists of roles and responsibilities in this section have been created by RHFL and reflect the likely tasks that team members have to perform. Disaster Recovery Team members are responsible for performing all of the tasks mentioned there on. In some disaster situations, Disaster Recovery Team members may also be called upon to perform tasks not described in this section.

4.1 Disaster Recovery Lead

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role is to guide the disaster recovery process and all other individuals involved in the disaster recovery process have to report to this person in the event that a disaster occurs at RHFL regardless of their department and existing managers. All efforts are to 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 is not a member of other Disaster Recovery group.

Role and Responsibilities

- Makes the determination that a disaster has occurred and trigger the DRP and related processes.
- Initiates the DR Call Tree.
- Be the single point of contact for and overseer for all of the DR Teams.
- Organizes and chairs regular meetings of the DR Team leads throughout the disaster.
- Presents to the Management Team on the state of the disaster and the decisions that need to be made.
- Organizes, supervises and manages all DRP test and authors all DRP updates.

Contact Information

Contact Designation	Role	Home Phone Number	Mobile Phone Number
Chief Development Officer	**Disaster Recovery Lead**	**Annexure - I**	**Annexure - I**

4.2 Disaster Management Team

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

Role & Responsibilities

- Set the DRP into action 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.
- Get the DR site ready to restore business operations.
- Ensure that the DR 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 RHFL is back to business as usual, this team is required to summarize any and all costs and provide a report to the Disaster Recovery Lead summarizing their activities during the disaster.
- Also document the steps taken to bring back normalcy.

Contact Information

Contact Designation	Role/Title	Home Phone Number	Mobile Phone Number
CIO	**Disaster management Primary Team Lead**	**Annexure - I**	**Annexure - I**
CTO	**Disaster management Secondary Team Lead**	**Annexure - I**	**Annexure - I**

4.3 Administration department Team

The Administration department Team is responsible for all issues related to the physical facilities that support Datacenter operations. This is the team that is responsible for ensuring that the required facilities are provided 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

- Ensure that transportation is provided to all employees working out of the DR Center.
- Assess, or participate in the assessment of, any physical damage to the Data Center.
- 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 that all employees are provisioned in an appropriate timeframe.
- This team is required to maintain a log of where all of the supplies and equipment were used.
- Ensure that appropriate resources are provisioned to rebuild or repair the main facilities in the event that they are destroyed or damaged.

Contact Information

Contact Designation	Role	Home Phone Number	Mobile Phone Number
GM -Admin	Facilities Team Head	Annexure - I	Annexure - I
AGM-Admin	Facilities Team Coordinator	Annexure - I	Annexure - I

4.4 Network Team

The Network Team is responsible for assessing damage specific to any network infrastructure and for provisioning data and network connectivity including WAN, LAN, Broadband etc., within the enterprise as well as data connections with the branches. They are 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 DR Center; the team has to identify which network services are not functioning at the Data Center.
- If multiple applications are impacted, the team has to prioritize the recovery of applications in the manner and order that has the business impact.
- If network services are provided by third parties, the team has to communicate and co-ordinate with these third parties to ensure recovery of connectivity.
- In the event of a disaster that does require migration to DR Center, the team has to ensure that all network services are brought online at the secondary facility
- Install and implement any tools, hardware, software and systems required in the DR Center.
- Ensure connectivity between Datacenter and Branches are UP and running.
- Analyze and document the Root Cause for the network failure.
- Update the status and progress to the Disaster Management Team Coordinators.

Contact Information

Contact Designation	Role	Work Phone Number	Home Phone Number	Mobile Phone Number
AM – IT	Network Team Lead	Annexure - I	Annexure - I	Annexure - I
AM – IT	Network Team Member	Annexure - I	Annexure - I	Annexure - I

4.5 Server Team

The Server Team is responsible for rebuilding the server infrastructure required for RHFL to run its IT operations and applications in the event of and during a disaster. They are 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 DR center, the team has to identify which servers are not functioning at the Data Center.
- If multiple applications are impacted, the team has to prioritize the recovery of applications in the manner and order that has the business impact. Recovery includes the following tasks:
    - Assess the damage to servers.
    - Restart and refresh servers if necessary
- Ensure that secondary servers located in DR Center are kept up-to-date with system patches.
- Ensure that secondary servers located in DR Center are kept up-to-date with data copies
- Ensure that the secondary servers located in the DR Center are backed up appropriately
- Warranty details
- Vendor coordination

Contact Information

Contact Designation	Role	Home Phone Number	Mobile Phone Number
Manager – IT	Datacenter Team Lead	Annexure - I	Annexure - I
Manager - IT	Hardware Team Lead	Annexure - I	Annexure - I

4.6 Applications and Database Team

The Applications Team is responsible for ensuring that all Core Banking applications functions as required to meet business objectives in the event of and during a disaster. They are 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 DR center, the team has to identify which applications are not functioning at the Data Center.
- If multiple applications are impacted, the team has to prioritize the recovery of applications in the manner and order that has the 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.
- Ensure that secondary servers located in DR center are kept up-to-date with application patches.
- Ensure that secondary servers located in DR Center are kept up-to-date with data copies
- Install and implement any tools, software and patches required in the Data Center.
- Install and implement any tools, software and patches required in the DR Center.

Contact Information

Contact Designation	Role/Title	Home Phone Number	Mobile Phone Number
Manager - IT	Database Team Lead	Annexure - I	Annexure - I
Manager - IT	Application Team Lead	Annexure - I	Annexure - I

4.7 Senior Management Team

The Senior Management Team has to 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 ultimately report to this team.

Role & Responsibilities

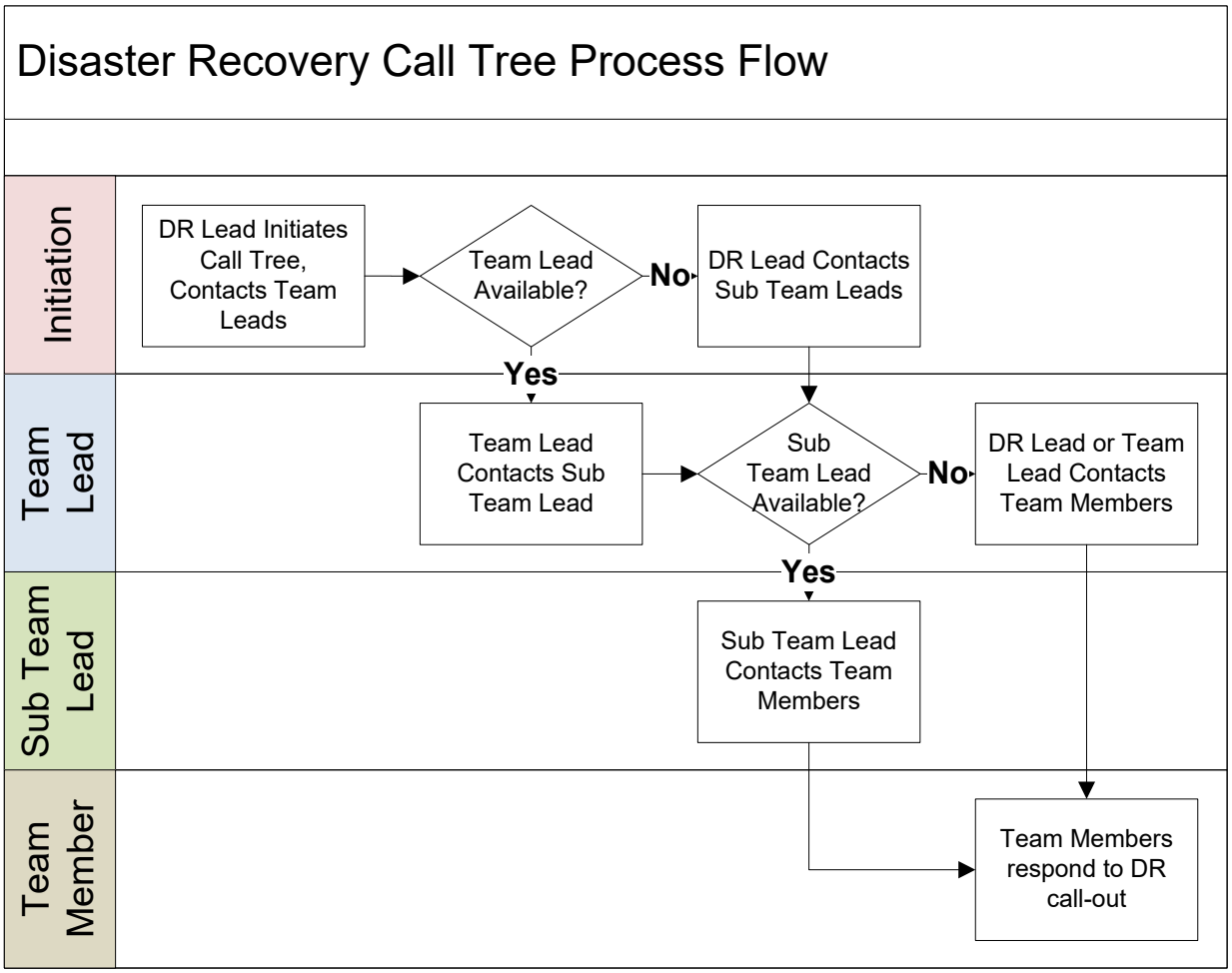
- Ensure that the Disaster Recovery Team Lead is held accountable for his/her role.
- Assist the Disaster Recovery Team Lead in his/her role as required.
- Make decisions that will impact the company. This can include decisions concerning:
    - Rebuilding the Datacenter.
    - Significant hardware and software investments and upgrades.
    - Other financial and business decisions.

Contact Information

Contact Designation	Role	Home Phone Number	Mobile Phone Number
MD	Senior Management Team	Annexure - I	Annexure - I
CDO	Senior Management Team	Annexure - I	Annexure - I

5. Disaster Recovery Call Tree

- In a disaster recovery or business continuity emergency, time is of the essence, so RHFL has to make use of a Call Tree to ensure that appropriate individuals are contacted in a timely manner.
- The Disaster Recovery Team Lead calls Disaster Management Team Leads and initiates the DR Process.
- Disaster Management Team Leads call all the respective team Leads and initiate their roles.
- Respective team leads enable their team to initiate the DR process.



Disaster Recovery Call Tree – Annexure – II

6. Data and Backups

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

Data in Order of Criticality – Annexure III

7. Communicating During a Disaster

In the event of a disaster RHFL needs to communicate with various parties to inform them of the effects on the business, surrounding areas and timelines. The Communications Team is responsible for contacting all stakeholders. Disaster Management Team Lead shall communicate all information related to the Disaster and the Recovery process to all the Respective Communication Team Leads.

7.1 Communicating with the Authorities

The Communications Team's first priority is 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.
- Expected timelines.

Authorities Contacts – Annexure IV

7.2 Communicating with Employees

The Communication Team's second priority is to ensure that the entire company has been notified of the disaster. A senior officer from each department shall be assigned as Communications Team Lead. Communication team Lead is responsible for updating his subordinates in case of Disaster. For all staff members, the respective Communication Team Lead will be the Single point contact for any queries related to a Disaster. Communication Team Lead shall have his entire team member Contacts handy.

- E-mail (via official e-mail where that system still functions)
- Employee's home Landline number
- Employee's mobile phone number
- Postal address
- whatsapp

The employees are needed to be informed of the following:

- Whether it is safe for them to come to the office
- Where they should go if they cannot come to the office
- Which services are still available to them
- Work expectations of them during the disaster

Communication Team Lead Contacts

Communication Team Lead Contacts		
Designation	**Department**	**Mobile Number**
GM	HR, Training & Admin	Annexure - V
GM	Credit/Legal	
GM	Credit Review/CDR/Offsite/Recovery (other than TN)	
GM	Sales/Insurance/PPD/CSD	
GM	Operations/Recovery (TN)	
GM	IT/MIS	
GM	Accounts & Finance/ Investor relations	
CS	CS/SEBI & Regualtory Compliance/Secretarial/CSR	
DGM	Risk	
DGM	RBI & NHB Compliance	
DGM/HIA	Internal Audit/Vigilance/Staff Accountability	
AGM	CISO	

7.3 Communicating with Vendors

After all of the organization's employees have been informed of the disaster, the Communications Team is 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 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.

Crucial Vendors – Annexure VI

8. Dealing with a Disaster

If a disaster occurs in RHFL 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) Assessment of current and prevention of further damage.
4) DR Center activation.

8.1 Disaster Identification and Declaration

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

- First hand observation.
- System Alarms and Network Monitors.
- Environmental and Security Alarms in the Data Center.
- Security staff.
- Facilities staff.
- 3rd Party Vendors.
- Warnings from Government agencies like Meteorological department

Once the Disaster Recovery Lead has determined that a disaster had occurred, 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 in the Data Center at the time of the disaster has been evacuated to safety.

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.

8.2 DRP Activation

Once the Disaster Recovery Lead has formally declared that a disaster has occurred he has to initiate the activation of the DRP by triggering the Disaster Recovery Call Tree. The following information is to 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

If the Disaster Recovery Lead is unavailable to trigger the Disaster Recovery Call Tree, that responsibility shall fall to the Disaster Management Team Lead. If Disaster Management Team lead is also not available, then **Facilities Team Head** should take lead.

Assessment of Current and Prevention of Further Damage

Before the employees from RHFL can enter the Data Center after a disaster, appropriate authorities must first ensure that the premises are safe to enter.

The first team that is allowed to examine the primary facilities once it has been deemed safe to do so is the Admin Team. Once the Admin 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 are allowed to examine the building. All teams are required to create an initial report on the damage and provide this to the Disaster Recovery Lead within a week 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 RHFL'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.

8.2 DR Center Activation

The DR Center is formally activated when the Disaster Recovery Lead determines that the nature of the disaster is such that the Data Center is no longer sufficiently functional or operational to sustain normal business operations.

Once this determination is made, the IT Team has to be advised to bring the DR Center to functional status. After that the Disaster Recovery Lead has to convene a meeting of various Disaster Recovery Team Leads. The next steps will include:

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 operations tasks outstanding/required at DR Center

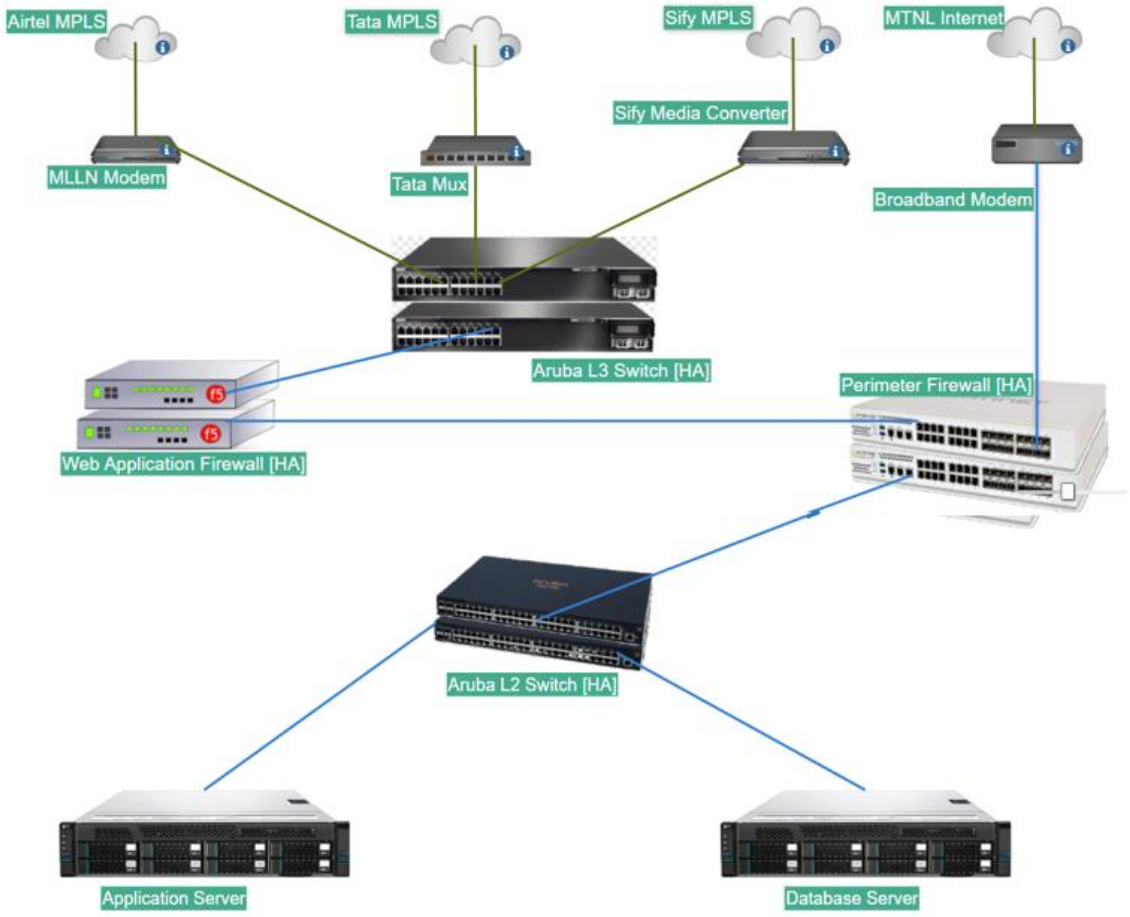
During DR Center activation, the Admin, Networks, Servers, Applications and Operations teams need to ensure that their responsibilities, as described in the “Disaster Recovery Teams and Responsibilities” section of this document are carried out quickly and efficiently so as not to negatively impact the other teams.

9. Restoring IT Functionality

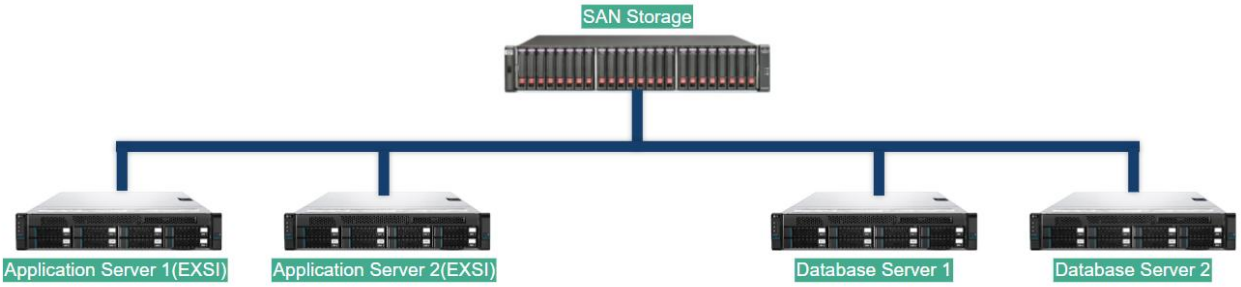
This section is to be referred frequently as it contains all of the information that describes the manner in which RHFL's information system can be recovered.

This section contains all of the information needed for the organization to get back to its regular functionality after a disaster has occurred.

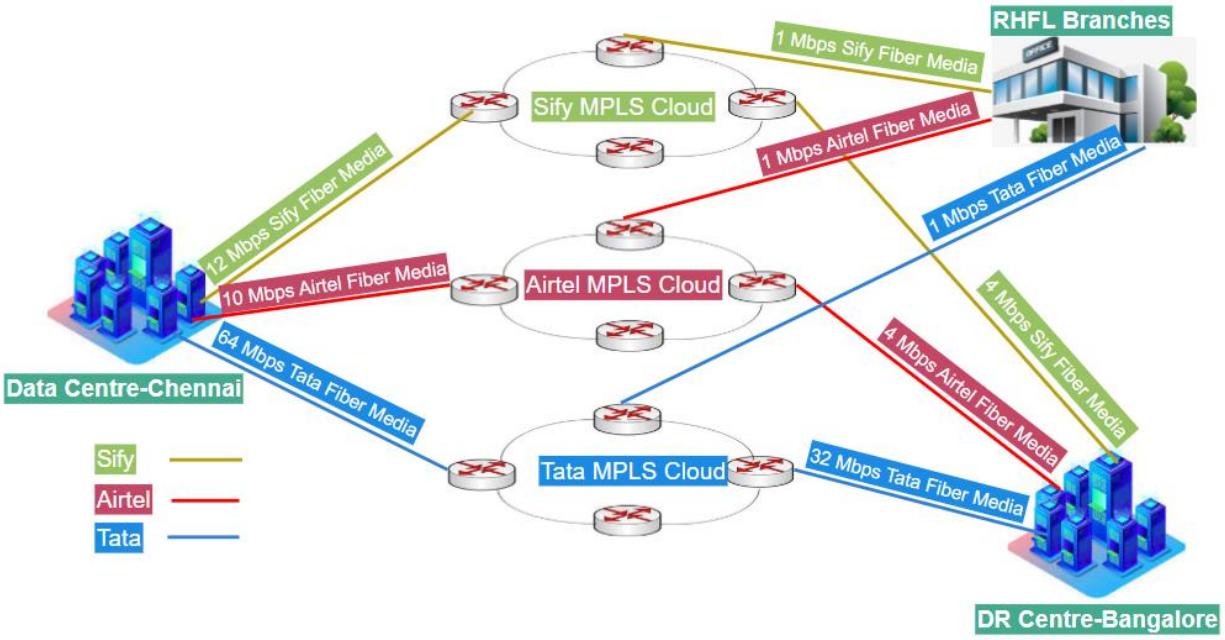
9.1 Network



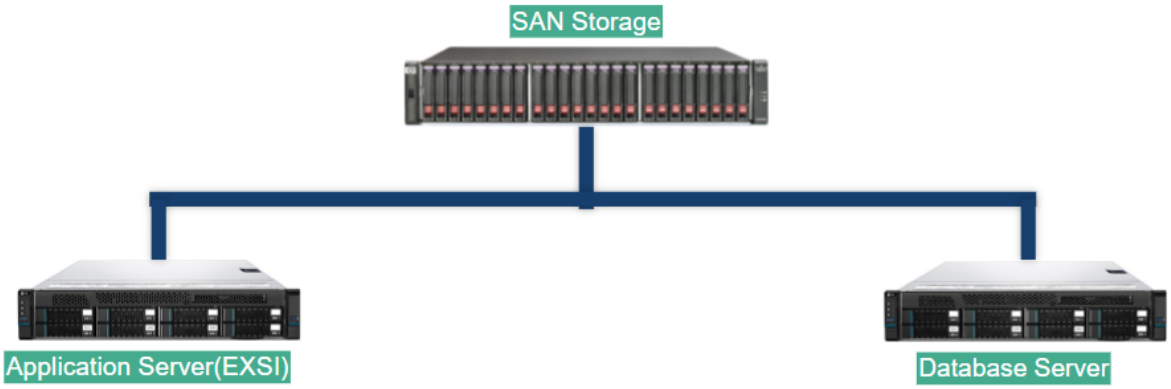
9.2 Servers



9.3 MPLS Connectivity



9.4 DRC SERVERS



10. 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 RHFL 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.

- Make Sure the DRP is Ready for a Disaster

Maintenance

The DRP will be updated once in a year 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.

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.

11. Testing

RHFL's IT Department is committed to ensuring that this DRP is functional. The DRP should be tested every Six months in order to ensure that it is still effective. Testing the plan will be carried out as follows:

Call Tree Testing

Call Trees are a major part of the DRP and RHFL requires that it is tested every Six months 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.

12. Business Continuity Plan

BCP forms a part of an organization's overall Business Continuity Management (BCM) plan, which is the "preparedness of an organization", which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business process, at an agreed level and limit the disaster impact of the people, process and IT infrastructure. Planning is the act of proactively working out a way to prevent, if possible, and manage the consequences of a disaster, limiting it to the extent that a business can afford.

12.1 BCP Head or Business Continuity coordinator

The DRP Lead shall be designated as the Head of BCP activity or function.

Roles and Responsibilities of BCP Head

- Determining how the institution will manage and control identified risks.
- Allocating knowledgeable personnel and sufficient financial resources to implement the BCP
- Prioritizing critical business functions.
- Designating a BCP committee who will be responsible for the Business continuity management.
- Review the adequacy of the institution's business recovery, contingency plans and the test results and put it up to the senior management.
- Should consider evaluating the adequacy of contingency planning and their periodic testing by service providers whenever critical operations are outsourced.
- Ensuring that the BCP is independently reviewed and approved at least annually;

- Ensuring staff members are trained and aware of their roles in the implementation of the BCP.
- Ensuring the BCP is continually updated to reflect the current operating environment.
- Prioritization of business objectives and critical operations that are essential for recovery.
- Business continuity planning to include recovery, resumption and maintenance of all aspects of the business, not just recovery, resumption and maintenance of all aspects of the business, not just the recovery of the technology components.

12.2 BCP Committee or Crisis Management Team

BCP committee consists of Head of the Departments of Credit, Admin, Accounts, Recovery, Risk, Legal and IT.

- To exercise, maintain and to invoke business continuity plan, as needed
- Communicating with relevant teams.
- Providing the facilities required for the Recovery team.
- Coordinating the activities of other recovery, continuity, and response teams and handling key decision-making.

12.3 Data Recovery Strategies

- Backups made to tape and sent off-site at regular intervals (preferably daily / weekly)
- High availability systems that keep both data and system replicated off-site, enabling continuous access to systems and data.
- Failover cluster of systems and data.
- Use of disk protection technology such as RAID
- Surge protectors—to minimize the effect of power surges on delicate electronic equipment Uninterrupted power supply (UPS) or backup generator to keep systems going in the event of a power failure.
- Fire preventions—alarms, fire extinguishers.
- Anti-virus software and security measures.

A disaster recovery plan is a part of the BCP. It dictates every aspect of the recovery process.

A disaster recovery plan must be a living document; as the Data Centre changes, the plan must be updated to reflect those changes.

Architecture Required

- **Data Centre solution architecture**
- **DRC solution architecture**

IT shall conduct performance and availability audit of the solutions deployed to ensure that the architecture is designed and implemented with **no single point of failure**.

IT shall audit the deployed architecture for all the mission critical applications and services and resolve the concerns that arise in a time bound manner.

IT shall periodically investigate the outages that are experienced from time to time, which are mini disasters that result in non-availability of services for a short span of time, systems not responding when transactions are initiated at the branch level, delivery channels not functioning for a brief period of time to ensure that the customer service is not affected.

IT shall ensure availability of appropriate technology solutions to measure and monitor the functioning of products. The issues detailed above have to be borne in mind while finalizing the Data centre architecture and the network architecture which are expected to have redundancy built in the solution with **no single point of failure.**

With reference to the data accessibility between DB server and SAN storage and also network architecture, it is recommended that RHFL built in redundancies as under:

- **Link level redundancy**
- **Path level redundancy**
- **Route level redundancy**
- **Equipment level redundancy**
- **Service provider level redundancy**

12.4 Backup site:

Backup site is an identified location where we can easily relocate following a disaster, such as fire, flood, terrorist threat or other disruptive event. This is an integral part of the disaster recovery plan and wider business continuity planning of RHFL. A backup site can be another location operated by the organization.

There are three main types of backup sites:

- cold sites
- warm sites
- hot sites

Differences between them are determined by costs and effort required to implement each. Another term used to describe a backup site is a work area recovery site.

1. Cold Sites: A cold site is the most inexpensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. The lack of hardware contributes to the minimal startup costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

2. Hot Sites: A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. Real-time synchronization between the two sites may be used to mirror the data environment of the original site, using wide area network links and specialized software.

3. Warm Sites: A warm site is, quite logically, a compromise between hot and cold. These sites will have hardware and connectivity already established, Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old.

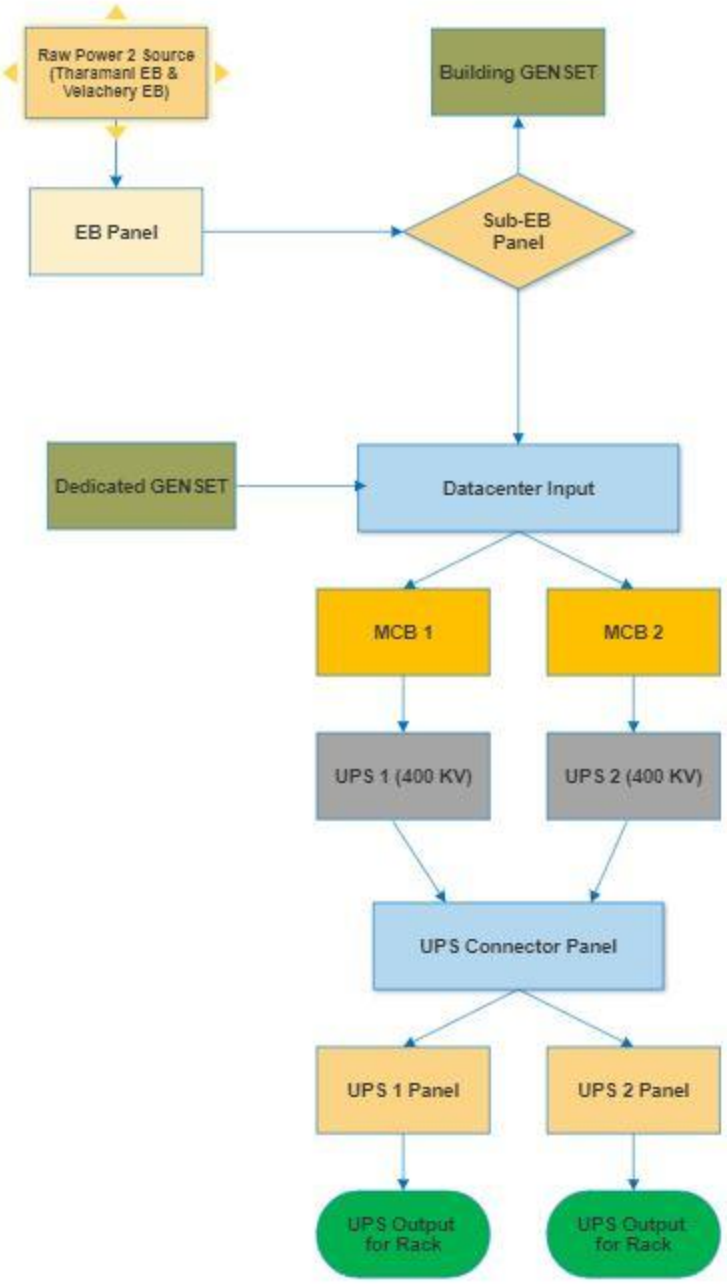
13. Recovery Plans:

1. Power Failure
2. Air Conditioner Failure
3. Network Failure
4. Server Failure
5. Application Failure
6. Database Failure
7. Natural Disaster

13.1 Power Failure Recovery

- All data center devices with dual source power input capability are connected to two different UPS sources.
- Devices with single power input capability are provided uninterrupted power using N+X parallel redundancy as shown above.
- Each 400 KVA UPS can provide power backup up to 25 minutes in case of power failure.
- As per current setup, if raw power fails, GENSET will switch ON in 15 seconds.
- GENSET can supply power up to 6 days.

Power Distribution to Datacenter



Scenario 1: Any one of the UPS fails:

- If any one of the UPS fails, all the DC equipment will run on single UPS without any interruption.

IMPACT:

No impact until both UPS goes down.

Recovery time:

06:00 hours

Scenario 2: RAW power fails:

- If raw power fails, GENSET will switch ON automatically within 15 Seconds and provides power to the Data Center.
- GENSET can supply power up to 6 days.
- If GENSET fails, UPS1 provides power for at-least 25 Minutes.
- If GENSET fails, UPS2 provides power for at-least 25 Minutes.

IMPACT:

No impact until both UPS fails.

Recovery time:

4:00 hours maximum

Scenario 3: Both the UPS fails:

- If both the UPS fails, Disaster Recovery Center will be made available for all branches.

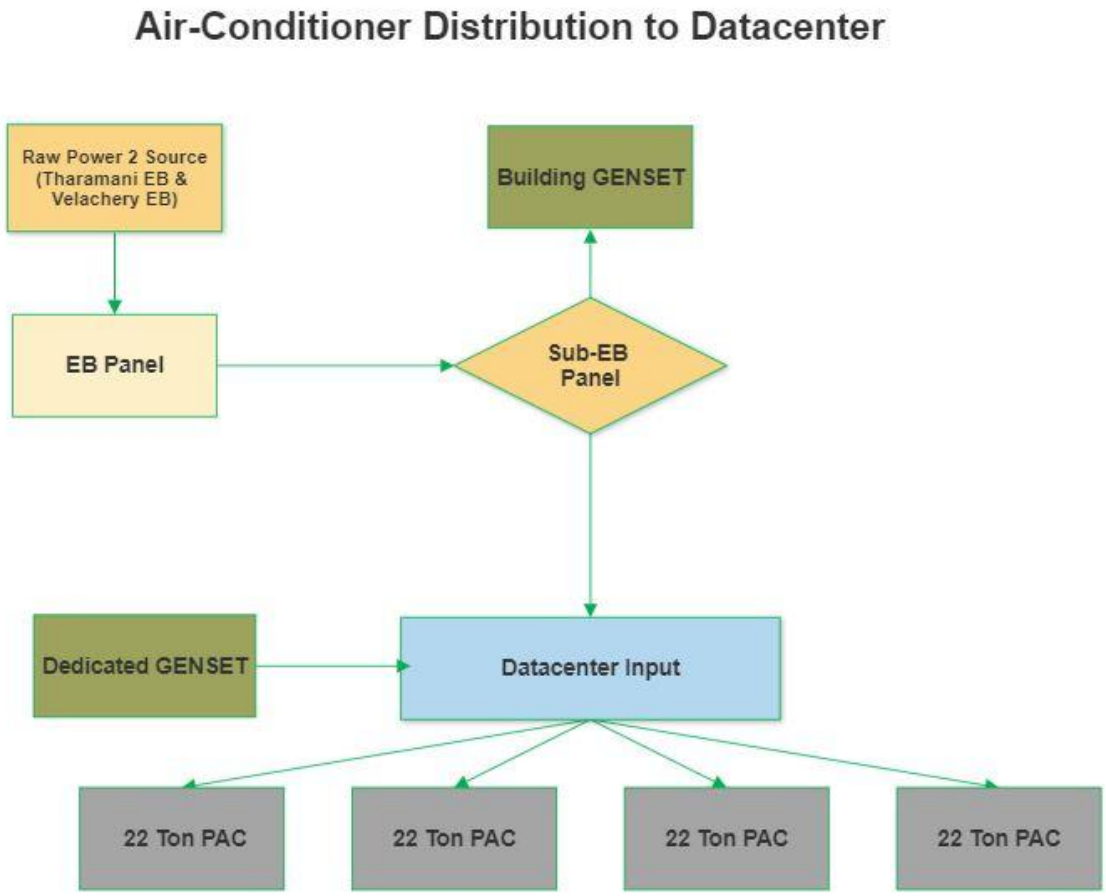
IMPACT:

Business impacted. DC will be shut down. All Branches have to be advised to use DR application.

Recovery time:

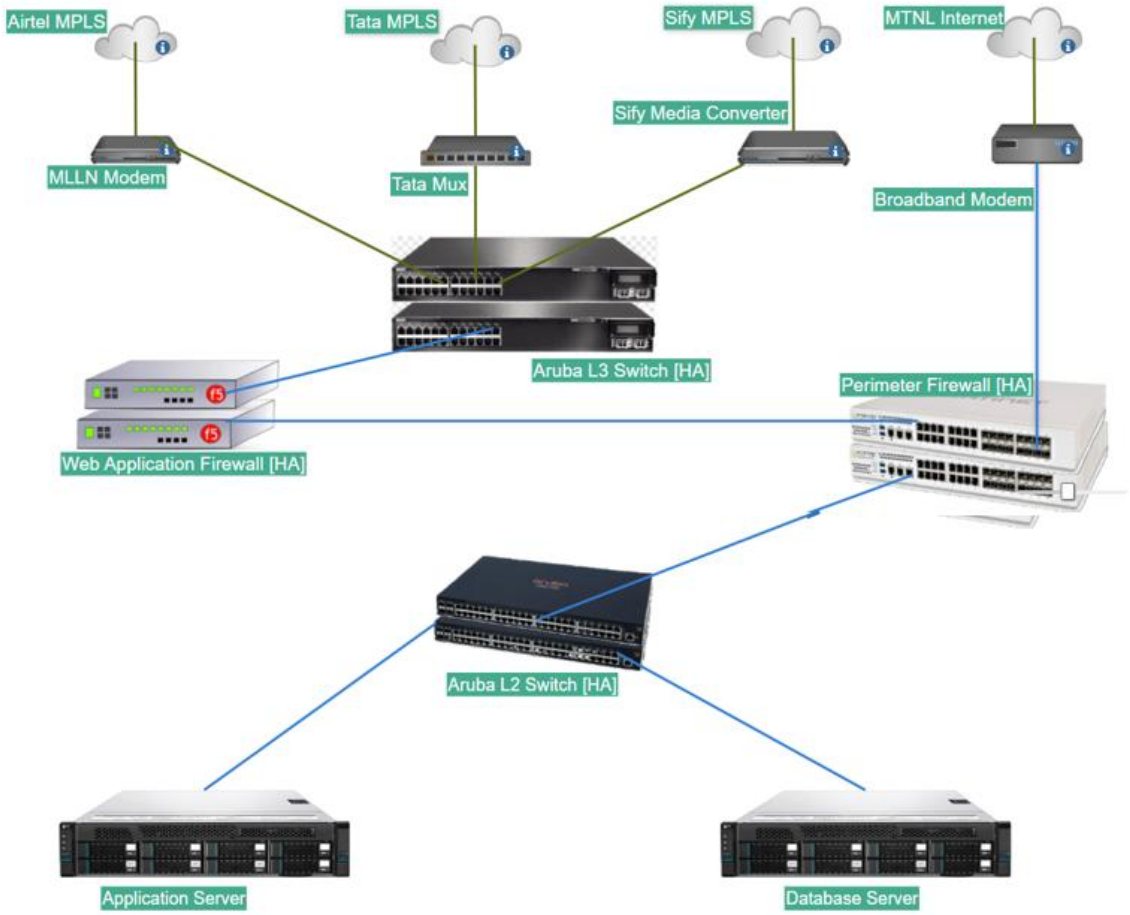
6:00 Hours Maximum.

13.2 Air Conditioner Failure Recovery



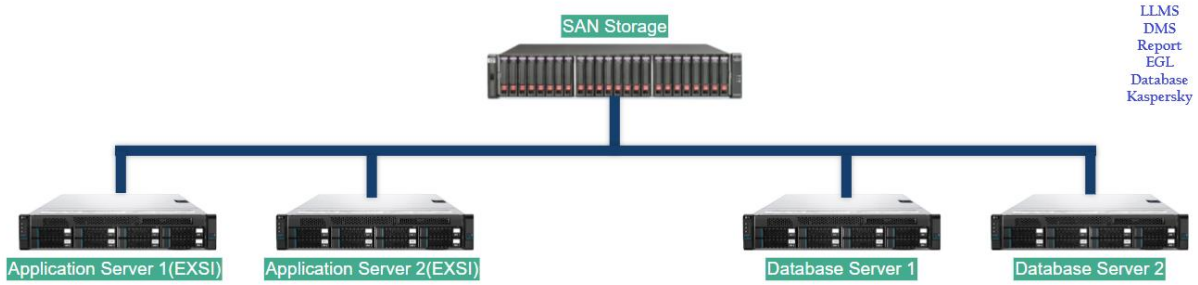
- Data Center has 4 Precision AC with 22 ton capacity each.
- Stabilized RAW power supply provided for all AC units.
- Timers are configured for all units to make sure at any time, AC is available in the Data Center.
- If raw power fails, GENSET will provide power automatically within 15 seconds.
- If entire power source fails, Data Center equipment shall be shut down and DR site will be enabled.

13.3 Network Failure Recovery



- Data Center has MTNL 100Mbps Internet Leased Line connection for internet purpose.
- Primary TATA 65Mbps, Airtel 100Mbps and Sify 12Mbps MPLS VPN links provide Intranet access to the Data Center from Branch locations.
- If anyone of the MPLS link fails, the branch can access Data Centre through Internet Leased Line with static IP address.
- If both MPLS and Internet Leased line are down, DR site will be enabled for Branches.

13.4 Servers Failure Recovery



Current DC Architecture has Hardware level redundancy for Application and Database servers.

- Database server is configured in cluster mode to attain redundancy at Datbase level(Oracle RAC Database).
- VSAN configured as RAID (1, 5) ensures data can be retrieved if any of the disks in server fails.
- DR site can be made available if VSAN fails.
- Primary Domain controller and Additional Domain controller provides redundancy for Domain controller.

13.5 Application Recovery

Applications used in RHFL

1. **Loan Life Cycle Management System (LLMS):**

   LLMS Application is running on two VMs (Virtual Machine) in two different host servers as active-active mode. Virtual Environment will provide redundancy at both Hardware level and Application level. If both the Application server fail, Branches will be advised to access LLMS from DR.

   Business Impact: High

   Recovery time: 8 hours.

2. **Enterprise General Ledger (EGL):**

   EGL Application is running on two VMs (Virtual Machine) in two different host servers as active-active mode. Virtual Environment will provide redundancy at both Hardware level and Application level. If both the Application server fails, Branches will be advised to access EGL from DR.

   Business Impact: High

   Recovery time: 8 hours

13.6 Database Recovery

Case- I: Any of the disks in SAN fails:

- Datacenter Administrator shall log a case with AMC vendor as per the matrix furnished below for replacing faulty disk.
- Branch operation will not be affected as two database server nodes are connected in RAC (Real Application cluster), since active connections of failure, nodes will automatically take over by another node.

Case- II: Entire SAN box fails:

- DR site will be enabled immediately for branches.
- Datacenter Administrator shall Log a case with AMC vendor for replacing the **SAN**, as per the matrix furnished below.
- Once the AMC vendor replaces the parts of SAN in DC, DBA shall copy the entire Database from DR database after EOD and rebuild the Database before BOD of next day.

CALL LOG PROCEDURE:

- Call log can be registered in the following two modes

  I. Toll Free Number – 1800 108 4746
  II. E-mail - in.contact@hp.com

- Following information should be furnished at the time of raising complaint.

  Device installed Address :

  Repco Home Finance Ltd,.
  C/o Software Technology Park of India,
  5, SH 49A, Tharamani, Chennai, Tamil Nadu 600113

  Device Details

  Name RHFL-PRIMERA-CHN-STG
  Model HPE_3PAR C630
  Serial # SGH131S14T

- Following contact Details of the person @ RHFL
  Name :Arunpandian
  E-mail Address : arunpandian@repcohome.com
  Mobile Number : 9629224720

- Vendor details : Solaris Computers
  - Sri. Balaji
  - 9840468003
  - balaji@solarisin.com

13.7 Natural disaster

13.7.1 Natural disaster

A natural disaster is a major adverse event resulting from the earth's natural hazards. Examples of natural disasters are floods, tsunamis, tornadoes, hurricanes/cyclones, volcanic eruptions, earthquakes, heat waves, and landslides. Other types of disasters include the more cosmic scenario of an asteroid hitting the Earth.

The following table categorizes some natural disasters and the first response initiatives.

Cause	Profile	First Response
Earthquake	The shaking of the earth's crust, caused by underground volcanic forces of breaking and shifting rock beneath the earth's surface	Shut off utilities; Evacuate building if necessary; Determine impact on the equipment and facilities and any disruption ; DR will be enabled
Fire (wild)	Fires that originate in uninhabited areas and which pose the risk to spread to inhabited areas	Attempt to suppress fire in early stages; Evacuate personnel on alarm, as necessary; Notify fire department; Shut off utilities; DR will be enabled
Flood	Flash flooding: Small creeks, gullies, dry streambeds, ravines, culverts or even low-lying areas flood quickly	Monitor flood advisories; Determine flood potential to facilities; Pre-stage emergency power generating equipment; DR will be enabled; Assess damage
Heat wave	A prolonged period of excessively hot weather relative to the usual weather	Listen to weather advisories; Power-off all servers after a graceful shutdown; Shut down main electric circuit usually

	pattern of an area and relative to normal temperatures for the season	located in the basement or the first floor ; DR will be enabled
Hurricane	Heavy rains and high winds	Power off all equipment; listen to hurricane advisories; Evacuate area, if flooding is possible; Checkwater and electrical lines for damage; Do not use telephones, in the event of severe lightning; DR will be enabled;Assess damage
Landslide	Geological phenomenon which includes a range of ground movement, such as rock falls, deep failure of slopes and shallow debris flows	Shut off utilities; Evacuate building if necessary; DR will be enabled;Determine impact on the equipment and facilities
Lightning strike	An electrical discharge caused by lightning, typically during thunderstorms	Power off all equipment; listen to hurricane advisories; Evacuate area, if flooding is possible; Check water and electrical lines for damage; Do not use telephones, in the event of severe lightning; DR will be enabled;Assess damage
Limnic eruption	The sudden eruption of carbon dioxide from deep lake water limnic	Shut off utilities; Evacuate building if necessary; Determine impact on the equipment and facilities and any disruption ; DR will be enabled
Tornado	Violent rotating columns of air which descent from severe thunderstorm cloud systems	Monitor tornado advisories; Power off equipment; Shut off utilities; DR will be

		enabled;Assess damage once storm passes
Tsunami	A series of water waves caused by the displacement of a large volume of a body of water, typically an ocean or a large lake, usually caused by earthquakes, volcanic eruptions, landslides, meteorite impacts and other disturbances above or below water	Power off all equipment; listen to tsunami advisories; Evacuate area, if flooding is possible; Check water and electrical lines for damage; DR will be enabled;Assess damage

13.7.2. Man-made disasters

Man-made disasters are the consequence of technological or human hazards. Examples include stampedes, urban fires, industrial accidents, oil spills, nuclear explosions/nuclear radiation and acts of war. Other types of man-made disasters include the more cosmic scenarios of catastrophic global warming, nuclear war, and bioterrorism.

The following table categorizes some man-made disasters and notes first response initiatives.

Example	Profile	First Response
Bioterrorism	The intentional release or dissemination of biological agents as a means of coercion	Get information immediately from Public Health officials via the news media as to the right course of action; if exposed, quickly remove the clothing and wash off skin; DR will be enabled;

Civil unrest	A disturbance caused by a group of people that may include sit-ins and other forms of obstructions, riots, sabotage and other forms of crime, and which is intended to be a demonstration to the public and the government, but can escalate into general chaos	Contact local police or law enforcement; If required, DR will be enabled;
Fire (urban)	Even with strict building fire codes, people still perish needlessly in fires	Attempt to suppress fire in early stages; Evacuate personnel on alarm, as necessary; Notify fire department; Shut off utilities; DR will be enabled;
Hazardous material spills	The escape of solids, liquids, or gases that can harm people, other living organisms, property or the environment, from their intended controlled environment such as a container.	Leave the area and call the local fire department for help. If anyone was affected by the spill, call the your local Emergency Medical Services line; DR will be enabled;
Nuclear and Radiation Accidents	An event involving significant release of radioactivity to the environment or a reactor core meltdown and which leads to major undesirable consequences to people, the environment, or the facility	Recognize that a CBRN incident has or may occur. Gather, assess and disseminate all available information to first responders. DR will be enabled; Establish an overview of the affected area. Provide and obtain regular updates to and from first responders.

END OF DOCUMENT