BERAR FINANCE LIMITED

BUSINESS CONTINUITY PLAN (BCP)/DISASTER RECOVERY (DR)

RECORD OF REVIEW:

Document Number	01
Revision Number	02
Document Classification	Internal
Originally formulated	March 30, 2021
Created by	Secretarial Department
Reviewed by	Risk Management Committee of the Company
Approved by	Board of Directors of the Company

Version No	Created/Modified Date	Created/modified by	Approved by
1	March 30, 2021	Secretarial Department	Board of Directors
2	April 28, 2022	Secretarial Department	Board of Directors

Introduction

Interruptions to business functions can result from major natural disasters such as earthquakes, floods, and fires, or from man-made disasters such as terrorist attacks, riots or war. The most frequent disruptions are less sensational—equipment failures, theft or sabotage.

Business Continuity Plan (BCP Plan), also known as Contingency Planning, defines the process of identification of the applications, customers (internal & external) and locations that a business plans to keep functioning in the occurrence of such disruptive events, as well the failover processes & the length of time for such support. This encompasses hardware, software, facilities, personnel, communication links and applications.

BCP plan is intended to enable a quick and smooth restoration of operations after a disruptive event. It includes business impact analysis, where each critical business function has been reviewed to determine the maximum allowable downtime before causing significant degradation to Berar Finance Limited (BFL) business operations. BCP plan development includes testing, awareness, training, and maintenance.

The BCP plan also defines actions to be taken before, during, and after a disaster.

Purpose

The plan has been developed to allow for Continuity of Business operations at a minimum level within BFL facilities at BFL offices (Head office & it's branches) in the event of an emergency.

BCP Objective

- Protect personnel, assets and information resources from further injury and/ or damage
- Minimize economic losses resulting from disruptions to business functions
- Provide a plan of action to facilitate an orderly recovery of critical business functions
- Identify key individuals who will manage the process of recovering and restoring the business after a disruption

- Identify the teams that will complete the specific activities necessary to continuecritical business functions
- Specify the critical business activities that must continue after a disruption
- Recover critical business functions and support entities
- Minimize damage and loss
- Resume critical functions at an alternate location
- Return to normal operations when possible.

BCP Committee Members and Contact details:

Name	Designation	Address	Mobile No.	Email ID
Sandeep Jawanjal	Director	19, Process Server Society, Swawlambi Nagar, Nagpur – 440022	9922200096	sandeep.jawanjal@ berarfinance.com
Amar Helonde	IT Manager	Plot No 345, Laxmi Nagar Nagpur – 440022.	09309580686	amar.helonde@ berarfinance.com
Sewak Bhishikar	Head: Business Development	Near Udaram Pehalwan, Golibar chowk, Pachpaoli road, Nagpur – 440018	09011558626	sewak.bhishikar@ berarfinance.com

Recovery Management Co-ordinator (RMC)

Someshwar Dhonge	Head: Collection	141, Naik Nagar, Near NIT Garden, Manewada Road, Nagpur - 440027	09011668943	someshwar.dhonge @berarfinance.com

In case of disaster happened at Branch level, respective branch head will act as Recovery Management Co-ordinator at branch level who will co-ordinate with RMC at the Head Office. The BCP Procedure is also sent to their mail ID. In case of emergency, the Committee members can retrieve the data from their mail for acting toward the disaster.

Procedure – Business Continuity Plan

This is a disaster recovery plan for BFL Data. The information present in this plan guides BFL operation & Data management and technical staff in the recovery of computing and network facilities and client data in the event that a disaster destroys all or part of the facilities. The primary focus of this BCP is to provide a plan to respond to a disaster that destroys or severely cripples BFL operation & Data computer systems. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

Disaster recovery plans are developed to span the recovery of data, systems, links and also include worst case scenarios such as:

1. Loss of access to facility
2. Loss of access to information resources
3. Loss of key personnel who are responsible for performing critical functions

Personnel

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even ifsome or all of the personnel are unavailable.

Salvage Operations at Disaster Site

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any storage media are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Recovery Site / Alternate site / Backup site

The DR Server Setup implemented at Virtual Galaxy Datacenter located near Mahatme Eye bank, Chhatrapati Nagar, Nagpur has been discontinued due to intermittent performance issues reported for the Production Server.

As per the IT infrastructure upgradation planned within a quarter, the DR setup will be implemented on Cloud along with a Secondary Storage system.

Purchase New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The BFL operation will rely upon emergency procurement procedures for equipment, supplies, software, and any other needs.

Begin Reassembly at Recovery Site

Salvaged and new components are reassembled at the recovery site. If vendors cannot provide a certain piece of equipment on a timely basis, then recovery personnel can make Last-minute substitutions. After the equipment reassembly phase is complete, thework turns to concentrate on the data recovery procedures.

Executive Management Team (EMT)

This group consists of members of BCP Committee, the Recovery Management Coordinator. The Executive Management Team makes the decision to mobilize the BFL's recovery organization. This decision is based upon their best judgmentin determining the extent and impact of the outage.

Recovery Management Co-ordinator (RMC)

The Recovery Management Coordinator (RMC) is the individual who manages the recovery operation. Throughout the recovery process, all recovery teams function under the supervision of the RMC.

IT Recovery Group

The IT Recovery Group manages the computer processing, internal/ external network connectivity and computer support requirements of the recovery effort.

Logistics Recovery Group

The Logistic Recovery Group manages the administrative and logistical requirements of the recovery effort, and performance those duties and activities not directly related to the recovery of business functions.

Corporate Communication Group

Corporate Communication Group is responsible for communication with all BFL employees and clients during recovery operations.

Berar Finance Limited's Business Continuity Process
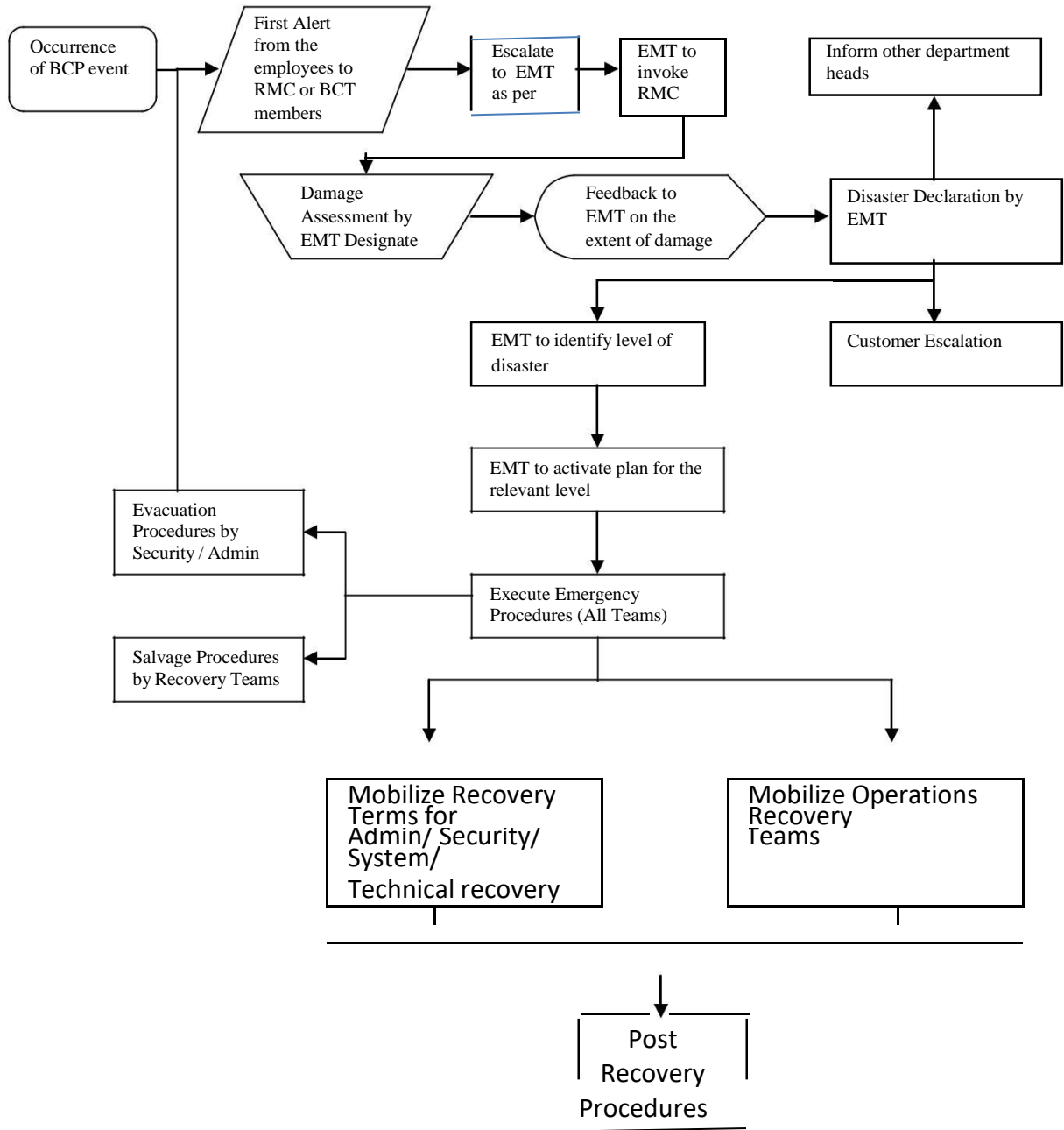
Restore Data from Backups:

Data can be restored from the daily backups available within office premises and outside as well. It can also be restored from other locations such as DR Failover server site in

case of any disaster.

1. Hardware Failure
2. Loss of data/software
3. Failure in communication link components
4. loss of power supply
5. loss / inaccessibility of other location

Geared for any eventuality

Server Hardware Failure	In case of any hardware failure vendor team will take care of the troubleshooting and issue resolution Server to be identified as critical and non-critical servers Critical servers to be configured for redundancy for power supply, disk mirroring etc. Redundancy to avoid /reduce impact of server failure.
Loss of Data/ Software	Almost Real-time data syncing in place Adequate backup maintained to recover loss of data daily & Daily backup of database is maintained Backup media to be tested at least once in two months Copies of backup maintained in secure offsite location.
Failure in data Circuits	For all communication problems at BFL's end: Network support outsourced to Virtual Galaxy. VG Network team will acknowledge and resolve the issue Equipments (router, connections hub) checked and rectified for problems detected Fully configured backup routers Alternate backup link facility in case of failure in dedicated link in one location
Loss of Power	Uninterrupted power supply through captive power plant available. UPS system backup for2 hrs. to avoid interruption in working
Loss / Inaccessibility of other location	Square up of position or important customers request can be managed from alternate locations.

PREVENTION

As important as having a disaster recovery plan is, taking measures to prevent a disaster orto mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created:

• **Fire**
• **Flood**
• **Earthquake**
• **Computer Crime**
• **Terrorist Actions and Sabotage**

Fire

The threat of fire in office premises is real and poses *a high risk*. The office premises are filled with electrical devices and connections that could overheat or short out and cause a fire. The computers within the facility also pose a target for arson from anyone wishingto disrupt BFL operations.

The offices are equipped with a fire alarm system. Ceiling mounted (ABC type) fire extinguishers are placed in visible and important locations throughout the building.

Flood

Only few of the branch offices are on ground floor and doesn't fall under declared Flood Zones, thus risk due to flood is very much limited. To prevent the offices from flood like situation, branch offices make sure the foundation has no cracks and coatings and sealants are applied on regular basis and Floodways are constructed to divert the excess water.

Earthquake

The threat of an earthquake in Nagpur and its braches is medium to low but should not be ignored. The Head office at Nagpur and majority branch offices are built to earthquake resistant standards so we could expect least damage from the predicted quake. An earthquake has the potential forbeing the most disruptive for this disaster recovery plan. Restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do large scale building repairs.

Computer Crime

Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before. Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from within.

To avoid Computer and cybercrimes, genuine firewalls and antivirus are used to protect private and financial information online.

All systems have security products installed to protect against unauthorized entry.All systems are protected by passwords. All users are required to change their passwordson a regular basis. All systems *should* log invalid attempts to access data, and *the* system administrator reviews these logs on a regular basis.

Physical security of the data storage area for backups is implemented. Standards have been established on the number of backup cycles to be retained and the length of their retention.

Policies and procedures are strictly enforced when violations are detected.

All the Berar Finance employees are instructed to follow the necessary guidelines for information security.

Terrorist Actions and Sabotage

Terroristic action and sabotage is potential risk under the circumstances on all the offices in big cities. To prevent such occurrence BFL has system in place whereby each office will permit entry on verification of personal details and due care is taken to provide adequate security. CCTV cameras has been installed, which gets monitored regularly.

Training

Training seminars addressing business continuity in are conducted on a regular basis. Also awareness programme is conducted to educate management and senior individualswho will be required to participate in the project.

The objectives of Business Continuity Planning training are:

- Train employees and management who are required to help maintain the BusinessContinuity Plan
- Train employees and management who are required to execute variousplan segments in the event of a disaster

<u>Testing and Evaluation</u>

The response to each threat situations is tested periodically to assess the preparedness of the organization to execute the recovery plans. Some of the threats that occur frequently,are tested in due course of business, hence are not tested specifically. Others however, require testing and for them a disaster scenario is assumed and the team representatives "walk through" the recovery actions checking for errors or omissions. Persons involved in the test include the Recovery Management Coordinator and members of various recovery teams.

An ongoing testing programme is established. However, special testing is considered whenever there is a major revision to BFL operation or when significant changes in hardware or communications environments occur. The Recovery Management Coordinator is responsible for analyzing change, updating impacts on the plan and for making recommendations for plan testing.

The Team Leaders and the Recovery Management Coordinator review the test results, discuss weaknesses, resolve problems and suggest appropriate changes to the plan.

An Effective recovery plan is a live recovery plan
Brief Description of BCP / DR Plan

Disruption	Availability			Impact		Recovery capability
	Processes	Personnel	Technology Assets	Financial	Operational	
Business processes (BP) at BFL level or at any office experience minor damage and will run at a sub-standard Level	Adequate	Adequate	Adequate	Low	Low	Immediate
BP at BFL level or at any office may not continue or may run on a sub-standard basis. Alternate equipment or routing of communication links may be required.	Adequate	Adequate	Adequate	Medium	Medium	Hours
Disaster resulting in the total shut down of central office premises leading to shut down of all business process, relating infrastructure and non- accessibility of people.	DR Failover Servers Setup (DB, Application & Remote Servers) Available	N.A. (24x7)	N.A.	N.A.	N.A.	N.A.
Major disaster resulting in a complete city wide destruction of service and damage to the Business Centre. Recovery will require the use of an alternate processing site as well as offsite office for employees over an extended periodof time.	Medium	Medium	Medium	Controllable	Controllable	Days