Business Continuity Policy

F.Y 2025 - 26

Introduction

A business continuity plan (BCP) is a plan to help ensure that business processes can continue during a time of emergency or disaster. Such emergencies or disasters might include a fire, Natural calamities or any other case where business is not able to function as in normal conditions. Businesses need to look at all such potential threats and devise BCPs to ensure continued operations should the threat become a reality.

Why we need Business Continuity Plan?

Disaster might occur anytime, so we must be prepared. Depend on the size and nature of the business, we design a plan to minimize the disruption on account of disaster and keep our business remain continue.

Due to the advancement of Information Technology (IT), business nowadays depends heavily on IT. With the emergence of e-business, many businesses can't even survive without operating 24 hours per day and 7 days a week. A single downtime might means disaster to their business.

Therefore the traditional Disaster Recovery Plan (DRP), which focuses on restoring the centralized data center, might not be sufficient. A more comprehensive and rigorous Business Continuity Plan (BCP) is needed to achieve a state of business continuity where critical systems and networks are continuously available.

When we need Business Continuity Plan?

We need Business Continuity Plan when there is a disruption to our business such as disaster. The Business Continuity Plan should cover the occurrence of following events:

a) Equipment failure (such as disk crash).
b) Disruption of power supply or telecommunication.
c) Application failure or corruption of database.
d) Human error, sabotage or strike.
e) Malicious Software (Viruses, Worms, Trojan horses) attack.
f) Hacking or other Internet attacks.
g) Social unrest or terrorist attacks.
h) Fire
i) Natural disasters (Flood, Earthquake, Hurricanes etc.)

Procedure – Business Continuity Plan

This is the disaster recovery plan for DMFL. The information present in this plan guides DMFL 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 DMFL 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

Since the Company has purchased cloud space and at present the working of our Jaguar system is operational through the cloud, instead of depending upon alternate servers, hence mitigating the maximum level of IT risk.

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 if some or all of the personnel are unavailable. In such emergent circumstances the in charge of disaster recovery system (IT Manager) is fully empowered to acquire/use any staff member of any section/ department of the company to make the functioning of the companies system normal.

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 Five offices spread across 3 states in India. Each site is equipped to provide similar working environments as other centers. The offices are interconnected with redundant leased lines and LAN network. The alternate site/ backup site is located at E-8 Geeta Nagri Bijnor Uttar Pradesh.

Purchase New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The DMFL 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, the work turns to concentrate on the data recovery procedures.

Restore Data from Backups:

Data can be restore from other locations in case of any disaster

Potential Causes of service interruptions:

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	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	Adequate backup maintained to recover loss of data Weekly backup of database 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 Company's end : Equipment's (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 UPS system. To avoid interruption in working.
Loss / Inaccessibility of other location	System operations can be managed form alternate locations.

PREVENTION

As important as having a disaster recovery plan, taking measures to prevent a disaster or to 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

The threat of fire in office premises is real and poses a high risk. The building is 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 wishing to disrupt Company operations.

Hand-held fire extinguishers are placed in visible locations throughout the building. All Staff are trained in the use of fire extinguishers.

Flood

None of the offices are on ground floor except delhi office, thus risk due to flood is very much limited.

Cyclones and High Winds

Most of the offices are located in the areas where Cyclones and High Winds are very much limited.

Earthquake

The threat of an earthquake in the areas where offices are located are medium but should not be ignored. Buildings in our area are built to earthquake resistant standards so we could expect least damage from the predicted quake. An earthquake has the potential for being 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.

The preventative measures for an earthquake can be similar to those of a Cyclone. Even if the building survives, earthquakes can interrupt power and other utilities for an extended period of time.

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 all of our system access the server system and the data is store only the main server machine not in every system. DMFL is using a Complete Antivirus product to manage & secure the main server machine.

Terrorist Actions and riots

Terroristic action and riots is potential risk under the circumstances on all the offices in big cities. Our main offices (Admin Office & Head Office) have security guards. Every person is checked & his details are verified before enter in this office. Every major points of office is under CCTV surveillance.

Outsourcing service

In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, DMFL retains an appropriate level of control over their outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of DMFL and its services to the customers.

Service provider of the DMFL ensures that DMFL able to isolate information, documents and records and other assets. In appropriate situations, DMFL can remove, all its assets, documents, records of transactions and information given to the service provider, from the possession of the service provider in order to continue its business operations, or delete, destroy or render the same unusable.

Testing and Evaluation Data

Drill

Complete Data restoration process has been done on half yearly basis and testing of back up data is also done immediate very next day of the drill.

Brief Description for Business Continuity

Disruption	Availability	Impact	Recovery Time Taken
Business process facing minor issue with Networking	Instant	Low	Immediate
Issue with ISP	Instant	Low	Immediate
Condition of riot or Curfew, Internet down from government side	Run system with Cloud Server	Controllable	At the earliest possible, keeping in view the prevailing situation.
Power Failure	Time Taken	Controllable	-do-
Server Shut Down or Crash	Instant with Backup Server	Low to Medium	Immediate being a cloud facility holder
Hard Disk Failure	Instant as Server with Raid Technology	Low to Medium	Minutes to Hours
Loss of Data or Data Corrupted from Virus	Time Taken	Depend on the Loss	Minutes to Hours

For Dhara Motor Finance Limited

Gajendra Singh
Managing Director

G.S.Chauhan
Whole Time Director