BUSINESS CONTINUITY PLAN (BCP)

I. Introduction

This policy focuses on sustaining the organization during and after disruption. This policy ensures that the Our Business Continuity Management arrangements are developed and implemented in a safe, prioritized and structured manner with the commitment of the senior management team. This policy refers to a coordinated strategy involving plan, procedures and technical measures that enable the recovery of process after disruption.

Preparation for, response to, and recovery from a disaster affecting the operations requires the cooperative efforts of many recovery teams comprising of members from support groups and the functional areas supporting the operations. This document records the Plan that outlines and coordinates the efforts of various recovery teams. For use in the event of a disaster, this document identifies the recovery facilities that have been designated as backups if the primary functional areas are disabled and critical business processes to be accommodated in the recovery facilities.

II. Aim

To develop, implement and manage a robust and effective Business Continuity Policy to protect our organization's operations, including our stakeholders such as employees, visitors etc.

III. Purpose

The purpose of the Business Continuity Policy is to provide an effective documented framework and a process to manage critical activities & their dependencies in case of an emergency.

The objectives of the Business Continuity Policy are:

- To mitigate the possible impact of an interruption to the activities
- To recover processes at identified recovery facilities
- To meet the Recovery Time

IV. Scope

The Business Continuity Policy does not address specific disaster events; it is written for a generic situation, which assumes that the primary site is suddenly inaccessible or must be vacated without warning.

This BCP does not address loss of some or majority or all personnel in a disaster. This policy is distributed to all employees of the organisation.

V. Assumptions

The following assumptions are made in the Business Continuity Policy:

- Key personnel and/or their backups identified in the plan are available
- Recovery location(s) and facilities, as required, are available that can handle the specified recovery activities
- Vital resources including backup media and other immediate requirements, identified in the strategy, required for BCP are available at the respective recovery location
- BCP shall not apply to non-recoverable situations such as global disaster
- BCP shall not be invoked for addressing day-today failures like link or system failure

VI. Plan Ownership and Maintenance

The Compliance Officer is the owner of the BCP document, and it is his/her responsibility is to keep it updated.

Ensuring that the Plan reflects ongoing changes to resources is crucial. This task includes updating the Plan and revising this document to reflect updates; testing the updated Plan; and training personnel. The Compliance Officer ensure that the Plan undergoes a more formal review to confirm the incorporation of all changes. Annually, the Board initiates a complete review of the plan, which could result in major revisions to this document. These revisions shall be distributed to all authorized personnel, who would then exchange their old plans with the newly revised plans.

VII. Roles and Responsibilities

Information Security

Our senior management has following ongoing responsibilities:

- Ensuring that recovery plans & procedures are in place.
- Ensuring that recovery is carried out effectively.
- Provide guidance and ongoing support.
- Periodic review of the plan.

Damage Assessment

Responsibilities include:

- Assess the extent of damage following the disaster
- Identifying possible causes of the disaster and their impact on the organization
- Estimate expected outage of disruption and predict downtime

Emergency Evacuation

Responsibilities include:

- Safe and speedy evacuation of personnel
- Ensure no personnel is left in the building
- Take a head count of their respective teams and notify

VIII. Containment Strategy

1. Response to emergency situations

The containment strategy deals with provisions for response to a business interruption caused by an emergency. The goal of the strategy is to provide for immediate response and minimize the need for decision-making during the emergency. In an emergency, the emergency plan will be activated.

2. Containment strategies

Containment strategies for each of the identified business interruption risks at primary data center are discussed below.

a. Hardware / Software failure

All the infrastructure at our registered office is commissioned in high availability mode or auto failure switching. Further, we work on a cloud server taken on lease agreement from the service provider for our data base. There is weekly backup of all the folders including configuration and the data files in the cloud server.

b. Virus infection

We use the Antivirus solution to prevent this situation from occurring. In case of virus outbreak we quarantine the entire system and up the standby system.

c. Natural Calamities

Our premise is situated at the Western coast of India which is low seismic zone. In case of major disaster, operation can be moved.

d. Fire accidents

Our premise is equipped with fire extinguisher for fire accidents.

e. Vandalism

The main entrance of our premises is protected by physical security and is under electronic surveillance. Entry to rest of the premises is restricted by access control system. Only our employees and authorized support group personnel are provided access into the premises.

f. Catastrophic events

In the case of Catastrophic events such as:

- Floods
- Earthquakes
- Storms
- Acts of terrorism
- Accidents or sabotage

All our services are based through an online platform. We have an online disaster recovery for our cloud Server.

g. Disaster Detection & Notification

The detection of an event, which could result in a disaster, affecting information processing systems in the organization, shall be reported to the on-duty officer and based on the severity of disaster he/she will report to the disaster recovery team.

Notification information shall include the following:

- Nature of emergency
- Loss of life or injuries
- Any known damage estimates
- Response and recovery details
- Where and when to convene for a briefing

Respective heads, business managers and team members will inform the clients accordingly about the plan of action.

IX. Testing Strategy

Testing is an essential element in the BCP effort and is performed to ensure that critical functions can, in fact, be accomplished according to the plan and that all components of the plan (i.e., personnel, hardware, software and administrative, etc.) function as expected. The Testing Strategy identifies the actions to be taken to ensure periodic testing of plans by regular basis, appropriate management review of all findings and timely correction of any identified deficiencies.