Jicadike.

TECH|FUTURE|READY|

BUSINESS CONTINUITY POLICY AND PROCEDUERS

Contents

1. 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 require 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.

Also, our business operations are through our franchise outlets which are spread across India. Hence, a disaster at any single town, district, city or state does not have a substantial impact on our business continuity.

For use in the event of a disaster, this document identifies the recovery facilities (Alternate site) that have been designated as backups if the primary functional areas are disabled and critical business processes to be accommodated in the recovery facilities.

This document identifies the Information security forum (ISF), Crisis Management Leader (CML) and other recovery teams along with their Roles & Responsibilities.

2. Aim

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

3. 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 of 30 mins

This Business Continuity Policy specifies the responsibilities of the Business Continuity Management Team and CML/IS Manager whose mission is to establish procedures to ensure the continuity of the organization operations.

4. 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 members of Information Security Forum.

5. 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-to-day failures like link or system failure

6. Plan Ownership and Maintenance

The Information Security Manager 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 CML and ISM are responsible for this comprehensive maintenance task.

The Business Continuity Management Team Coordinators ensure that the Plan undergoes a more formal review to confirm the incorporation of all changes. Annually, the CML 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.

7. Roles and Responsibilities

7.1 Information Security Forum (ISF)

Information Security Forum consists of Our senior management including Head Process, Information Security Manager and 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.
- BCP Project sponsorship.

7.2 Information Security Forum Operations

CML along with ISM are responsible for maintenance of BCP. Information Security Forum Operation responsibilities include:

- Guide CML from BCP initiation through recovery phase
- Ensure recovery is carried out effectively and securely
- Monitor situation and reports to ISF

7.3 Damage Assessment

Damage Assessment consists of Administration department functions of the organization.

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
- Notify ISM and ISF of the finding

7.4 Network Recovery Team

Network Recovery Team will carry out network recovery activity and team's responsibilities include:

- Replicating data center network and communications hardware at the recovery site
- Maintaining and administering networking infrastructure at the recovery site
- In case of disaster situation up the recovery site and route the traffic.

7.5 System Recovery Team

System Recovery Team will carry out system recovery activity and team's responsibilities include:

- Replicate data center's environment including hardware and software platform at the recovery site.
- Maintaining and administering hardware infrastructure and software platform at the recovery site.
- Regular restoring of the data from the periodic backup taken at DC
- In case of a disaster make the system live at the recovery site

7.6 Administrative Support Team

Administrative Support Team consists of members from the Administration function. Responsibilities include:

- Transportation of employees
- Procurement of necessary office and computer supplies
- Packaging and shipping of backup media
- Transportation of required IT equipment like servers, routers, workstations etc.
- Building perimeter security at both the affected primary site and recovery site

7.7 Emergency Evacuation Team

The Security Coordinators of each function and the Administration function head form the Emergency Evacuation Team.

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

8. Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

RTO and RPO are two important parameters of a Business Continuity Plan. RTO/RPO serves as essential business metrics for our internal teams to ensure that minimal data loss occurs in case of any disruption and there is optimal data backup available. While RTO/RPO depends on the criticality of data types, we target to maintain recovery time objective (RTO) and recovery point objective (RPO) of 48 hours and 2 hours, respectively, unless a lower minimum is provided by any of our partners/regulators in respect of any particular application.

9. Recovery of all major Services

9.1 Recovery Plan

We have the Disaster Recovery site at a datacenter in different geographies in different seismic zone where we make replica of complete environment of primary data center.

10. Containment Strategy

10.1 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.

10.2 Containment strategies

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

10.2.1 Link failure

We maintain redundancy for every connectivity link with auto failover switching. Our IT team would ensure that the link performance and link utilization is monitored. All the details of uptime and downtime will be consolidated and shown in the regular report, which can later facilitate follow-up actions.

If the downtime exceeds the limit identified in the service level agreement, we will follow up with the service provider and seek preventive and corrective actions.

10.2.2 Hardware / Software failure

All the infrastructure at our primary data center is commissioned in high availability mode or auto failure switching. Our IT team follows the best practice of regular backup of all the services including configuration and the data files of the production servers. DR team shall verify the backup to ensure readiness of backed up data for restoration at DR site in case of disaster.

10.2.3 Virus infection

Our network is closed and physically isolated from rest of the world except pre-defined network traffic. The physical access to the servers is strictly monitored. The servers are in the rack and the access of the same is given only to the identified IT operation Engineers. We use the best-in-class Antivirus solution to prevent this situation from occurring. In case of virus outbreak we quarantine the entire system and up the standby system.

10.2.4 Natural Calamities

Our premise is situated at higher altitude in the Western coast of India which is low seismic and non-flooding zone. In case of major disaster, operation can be move to DR site.

10.2.5 Fire accidents

Our premise is equipped with state-of-the-art integrated building management system which gives advance alert for any disaster like fire and any other disaster.

10.2.6 Vandalism

The main entrance of our premises is protected 24/7 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.

10.2.7 Catastrophic events

In the case of Catastrophic events such as:

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

All Our product and services are based through an online platform. We have an online disaster recovery for our Servers.

Being a Technology driven company we require less of human intervention for our product and services. Hence any Catastrophic events will not have a major impact on our business.

10.2.8 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 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

Recovery measures shall be discussed and carried out based on intensity of the disaster. CML will assess the situation and inform the key people about the action plan. CML team will be put into action for the recovery of critical processes.

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

11. Testing Strategy

Purpose

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, logistical, and administrative, etc.) function as expected.

11.1 General Approach to Testing

The Testing Strategy identifies the actions to be taken to ensure periodic testing of DR plans by DR drill on regular basis, appropriate management review of all findings and timely correction of any identified deficiencies.

11.2 Frequency of various tests, establishment and evaluation of test success

DR Drill must be carried out on a quarterly basis to test the effectiveness of DR plan. The test does not need to invoke all components of the plan concurrently. If the linkages among components have been sufficiently established and tested, testing may be conducted at a component level.

12. ISO 22301:2019 Business Continuity Management System

ISO 22301 understands and prioritizes the threats to an organizations business with the international standard for business continuity. ISO 22301 specifies the requirements for a management system to protect against, reduce the likelihood of, and ensure that the organizations business recovers from disruptive incidents

Below are the benefits of ISO 22301 business continuity management:

- Identify and manage current and future threats to an organizations business
- Take a proactive approach to minimizing the impact of incidents
- Keep critical functions up and running during times of crises
- Minimize downtime during incidents and improve recovery time
- Demonstrate resilience to customers, suppliers and for tender requests