



BUSINESS CONTINUITY POLICY

This policy focuses on sustaining the organization during and after disruption. This policy ensures that the 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.

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. where reasonably practicable

Purpose and object

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 is to mitigate the possible impact of an interruption to the activities.

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 the related employees who are in charge of its execution.

Respective Teams in the organisation: -

1. Information Technology

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

2. Information Security

- Ensure recovery is carried out effectively and securely

3. Damage Assessment

- 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

4. Network Recovery Team

- Replicating data centre network and communications hardware at the recovery site
- Maintaining and administering networking infrastructure at the recovery site

5. System Recovery Team

- Replicate data centre'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

6. Administrative Support Team

- 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.

7. Emergency Evacuation Team

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