

BCP DR Policy, Procedure and Plan

Intellectual Property / Confidentiality Statement

The information in this document has been made available to Polycab India Limited on the strict understanding that it, or the information herein, will not be shown, read, or passed to any person who is not a current employee of POLYCAB. This Policy has been developed by Polycab India Limited and its subsidiaries (POLYCAB) and is strictly confidential and applicable to all POLYCAB employees.

Document Approval:

This document has been approved by below-mentioned authorities.

Sr. No.	Name	Designation	Date	Signature & Approval Status
1	Mr. Gyan Pandey	Chief Digital and Information Officer (CDIO)	30-Sep-26	Approved
2	Mr. Pradipta Patro	Chief Information Security Officer (CISO)	30-Sep-26	Approved

Document Abstract:

This document specifies guidelines to address business continuity and IT disaster recovery requirements in Business Technology and IT Operations.

Document Title	Business Continuity Disaster Recovery Policy
Document Classification	Internal Revision No. 1.0
Document Publish	30 th Sep 2026
Latest Review Date	30 th Sep 2026
Review Cycle	Yearly
Review Next Review Date	01 st Oct 2027
Document Ownership	CISO
Document Author	CISO
Document Change Reviewers	CDIO
Document Circulation List	All Approvers, All Employees

28. BCP DR Policy

Revision History				
No.	Version	Date of Change	Author Revision	Description
1	V1.0	30 th Sep 2026	Sanket Mhatre	New document

Contents

1. Introduction.....	4
2. Scope and Applicability.....	4
3. Purpose.....	4
4. Roles and Responsibilities	4
a. BCP Steering Committee	4
.....	5
5. Business Continuity Procedure	7
a. Business Impact Analysis.....	7
b. Risk Assessment.....	8
c. Strategy Development	8
6. Description of recovery strategies.....	8
7. Plan Design (Business Continuity Plan)	10
8. Testing & Training	10
9. Maintenance & Continuous Improvement	11
10. RTO & RPO For Applications	Error! Bookmark not defined.
11. Testing Scenarios	11
12. BCP / DR for IT Service Outsourcing.....	12
13. Policy Exception.....	12
14. Policy Compliance.....	12
15. Review and Update	12
16. Annexure	12
17. Control Reference.....	13

1. Introduction

A Business Continuity Planning (BCP) and Disaster Recovery (DR) Policy is essential for ensuring that an organization can continue operating during and after disruptive events, such as natural disasters, cyber-attacks, or system failures. The BCP focuses on maintaining critical business functions and minimizing downtime, while the DR plan specifically addresses the restoration of IT systems and data after an emergency. This policy outlines the strategies, procedures, and resources required to prepare for, respond to, and recover from unforeseen incidents, ensuring that the organization can maintain its operations, protect its assets, and safeguard its reputation

2. Scope and Applicability

- This policy applies to all POLYCAB information, information systems and processing facilities that require continuous operation.
- All key personnel that are responsible for ensuring continued business operations across different businesses and department are covered under this policy.
- This policy is applicable to holding company and all subsidiaries of POLYCAB listed below.

3. Purpose

To integrate the information security management requirements of business continuity with other continuity requirements such as operations, staffing, materials, transport and facilities for enabling continued business operation in case of disaster.

4. Roles and Responsibilities

a. BCP Steering Committee

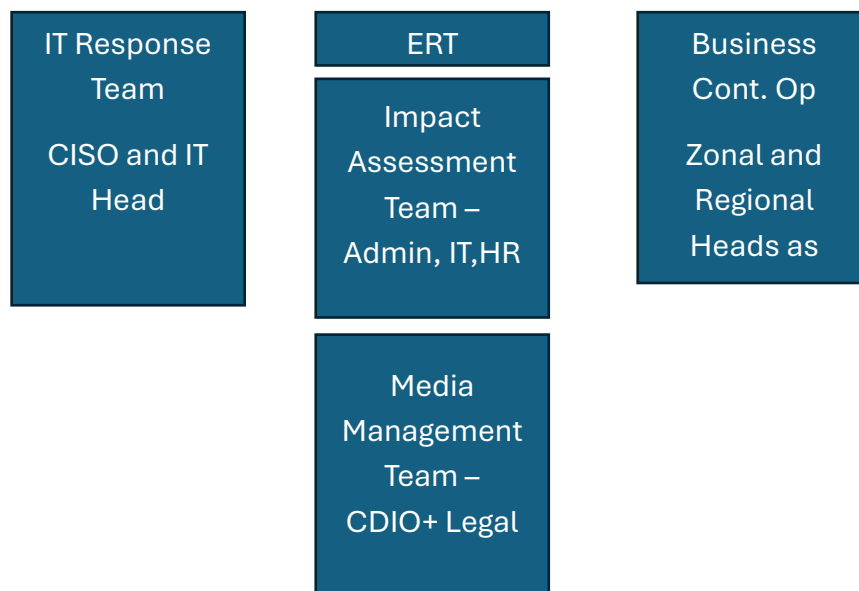
Composition of the BCP Steering Committee is as under:

CEO , also will be a Chairperson of the Committee

CDIO, CISO, Head - IT Infra Head, Head - IT Application, Head - Digital Applications, Head - ERP Systems, Head - Legal, CFO, Heads for B2B , B2C, FMEG , Exports, Engineering projects and Risk

b. Crisis Management Team

Crisis Management Team comprises of CxO, Op head, BU Heads (As required)

**Responsibilities**

- Overseeing development, implementation and maintenance of the DRBCP to ensure it accommodates changes to the POLYCAB environment (i.e. personnel, facilities, communications and equipment) Support the business continuity initiatives.
- Plan and direct POLYCAB's Response in case of crisis/disaster as per the DRBCP.
- Formation of Emergency Management Team and assigning responsibilities and guidance
- Review adequacy of resources in terms of people, IT infrastructure and Technology
- Key decision making in case of an actual disaster e.g. Declaration of Disaster, Activation of DRBCP, Relocation decision, etc.
- Authorize and approve all communication (internal/ external) with regard to the disaster. / Contingency (Refer Incident Management Policy)
- The DRBCP Committee would have the discretion to activate the DRBCP, depending on the situation and would exercise final discretion in the matter.

During Disaster/Emergency

- When communicated by the Chief BCP Coordinator of a disaster situation, evacuate the premises, if necessary and gather at the designated command centre.
- After assessing the situation determine which recovery teams are to be activated and which teams are to be placed on standby based on the instructions received from the DRBCP Committee.
- Monitor the progress of migration to recovery location from primary site.

28. BCP DR Policy

- Review important needs/ business priorities with recovery team leaders to ensure the most critical processes are recovered first.
- Ensure that each recovery team has been properly briefed on its recovery priorities by
 - Update DRBCP Committee on progress and challenges, if any
 - Ensure proper coordination between the recovery organization and vendors.
 - Manage contractual obligation with service provides, partners, distributors etc. to ensure smooth business operations during the crisis.
 - Keep track of accomplishments and misses in the recovery process for later review, audit and DRBCP updating.
 - Ensure availability of Disaster Recovery Procedures and SOPs.

During Business Resumption

- Authorize and approve business resumption to primary site post disaster.
- Monitor the progress of migration from recovery location to primary site.
- Update the stakeholders/ DRBCP Committee periodically on the status of business resumption
- Ensure proper communication between recovery organization, vendors and other external entities supporting business resumption process.
- After return to primary site, review the recovery log that is maintained by individual recovery teams
- This reporting shall be useful for coordinating an incident in progress and/or Ex-Post analysis which shall help in providing input for further updating the DRBCP.
- The company shall develop a comprehensive Business Continuity Plan and IT Disaster Recovery Plan. (BCP/DRP)
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan shall cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- BCP/DRP shall be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- Employees must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.
- The Process is applicable to all critical functions identified for continuity of business at such as
 - All business process and enabling functions of
 - All technical infrastructure
 - Corporate applications which cater to business operation requirements

28. BCP DR Policy

- Application / Business units with specific requirement for DR if any
- BCP/DR arrangements of critical vendors shall be incorporated in the service agreements and shall be reviewed

c. HR & Admin

- Tracking staff whereabouts and ensuring staff safety and welfare
- Contact staff and relay messages and confirm availability.
- Arranging catering, accommodation, staff rotation, etc.
- Ensuring security is enforced at the incident and any temporary recovery location.
- Facilitation of insurance claims and emergency payments/ purchasing.
- Redirection of mail and couriers.
- Staff Transportation, if required.

5. Business Continuity Procedure

Business Continuity Planning (BCP) ensures businesses can continue or immediately resume performing the critical business functions, which are the functions that support the organization's mission, comply with legal requirements, and support life-safety, under all circumstances. This includes natural, technological, and man-made incidents, as well as incidents that result in loss of access to parts of or an entire facility or loss of service due to equipment or systems failure. The Business Continuity Planning includes the ability to anticipate response actions following a myriad of incidents, improve the businesses performance of its critical business functions, and ensure timely recovery.

The Business continuity planning includes the following.

a. Business Impact Analysis

Business Impact Analysis (BIA) is a core part of business continuity planning—it identifies critical functions, evaluates how disruptions affect them, and helps organizations design recovery strategies to minimize downtime and financial loss.

Key Steps in Conducting a BIA**1. Identify Critical Processes**

- Map business functions (e.g., finance, IT, HR, customer service, production).
- Determine dependencies (systems, vendors, staff).

2. Assess Impact of Disruption

- Financial losses (e.g., missed revenue, penalties).
- Operational impact (e.g., halted production, delayed services).
- Regulatory/legal consequences (e.g., non-compliance fines).
- Different scenarios may be considered as below

3. BCP Scenarios and Management Plan

28. BCP DR Policy

Below will identify different types of threats and crisis that business continuity in .

Mentioned below are the scenarios which may trigger BCP activation and its management plan.

- Primary site is not accessible, but primary data center and DR site are available.
- Primary site is accessible, but primary data Centre is disrupted Trigger Event
- Primary site is accessible but both data center. i.e. Primary and DR site is disrupted.
- Trigger Event: Ransomware Response and Recovery Measures
- Any Plant/branch office is inaccessible.
- Cyber Incidents

Ref: Incident response, containment, recovery and preventive measures for various cyber crisis scenarios have been mentioned in detail in the Cyber Crisis Management Policy and Procedure, Incident Management Policy and Procedure

4. Define Recovery Objectives

- RTO (Recovery Time Objective): Maximum acceptable downtime.
- RPO (Recovery Point Objective): Maximum acceptable data loss.

5. Develop Mitigation & Recovery Strategies

- Replication, Backup systems for IT DR and
- Work from alternate suppliers, remote work arrangements for other BCP arrangements
- Communication plans for stakeholders.

b. Risk Assessment

Risk Assessment evaluates the likelihood of threats (cyberattacks, natural disasters, insider risks) and assesses vulnerabilities in systems, people, and processes. It produces a risk register with probability and severity ratings.

Refer to Risk Assessment Methodology and Risk Register/ Risk Assessment and Treatment plan for details of risks perceived by business continuity point of view.

c. Strategy Development

Based on Business Impact Analysis and Risk Assessment, Polycab shall design continuity strategies (redundancy, replication, backups, alternate sites, vendor diversification).

6. Description of recovery strategies

Based on the disaster scenarios, various recovery options have been identified for carrying out recovery of critical business processes.

To build resiliency in the recovery process it is recommended that each department selects two strategies.

28. BCP DR Policy

Below is a detailed description of each of the recovery strategies:

Recovery Strategies	Recovery Options	Description
Remote Access	Work from Home	Work from home is a strategy to carry out the tasks of the critical business processes of respective departments from home by using Remote Access. In this strategy the resources will be provided with Polycab provided Laptops with internet access (Data card / Wi-Fi), Virtual Private Network (VPN) access to carry out their critical tasks.
Displacement Strategy	Split Operations	In this strategy the workload of the department during normal operations is divided and the activities are carried out from two or more sites. The resources available at respective sites shall have adequate training and working understanding of the business processes. In case of any disaster situation where one of the sites is impacted, the operations shall be carried out from the remaining operational site.
Alternate Location	Use of Alternate Office Locations	Alternate location can be defined as an existing site held in readiness for use during invocation of Business Continuity Plan to continue the critical processes and tasks of Polycab. During any disaster situation where the primary Polycab location is not accessible / available, the alternate site can be used as alternate location to continue the operating business.
Cross Training	Training Plan	Resources from another location, are trained to perform critical processes of the affected

Recovery Strategies	Recovery Options	Description
		location. For example, resources from one of the Regional Office may be trained to perform one of identified critical processes at Head Office. Cross training as a recovery strategy requires identifying, equipping staff member who will be able to execute critical processes from their current work location in case of a disaster on behalf of the affected location.

Every department shall select a strategy or combination of the strategies in order to ensure the critical processes are resumed within their respective Recovery Time Objective (RTO's) and Recovery Point Objective (RPO's) at an agreed service level.

7. Plan Design (Business Continuity Plan)

- Documented procedures for response, recovery, and communication.
- Includes incident response, crisis communication, and escalation paths.
- Refer to IT Disaster Recovery Procedure and IT Disaster Recovery Plan for details

8. Testing & Training

- Simulation exercises, tabletop drills, penetration tests.
- Ensures staff know their roles and plans are practical.

Testing Techniques

The below are few of the illustrative techniques that can be used for BCP testing purposes:

1. Table-top testing for scenarios (discussing business recovery arrangements using example interruptions)
2. Simulations (particularly for training people in their post-incident or crisis management roles)
3. Technical recovery testing (ensuring information systems can be restored effectively)
4. Testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site)
5. Tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment)
6. Complete rehearsals (testing that the organisation, personnel, equipment, facilities and processes can cope with interruptions).

Simulation Testing:

It is when participants choose a specific scenario and simulate an on-location BCP situation. It involves testing of all resources: people, IT and others, who are required to enable the business continuity for a chosen scenario. The focus is on demonstration of capability, including knowledge, team interaction and decision-making capabilities. It can also specify role playing with simulated response at alternate locations/facilities to act out critical steps, recognise difficulties, and resolve problems.

Component Testing:

This is to validate the functioning of an individual part or a subprocess of a process, in the event of BCP invocation. It focuses on concentrating on in-depth testing of the part or sub-process to identify and prepare for any risk that may hamper its smooth running. The organisation must define frequency, schedule and clusters of Business Areas, selected for test after a thorough Risk and Business Impact Analysis has been done.

9. Maintenance & Continuous Improvement

Regular updates to reflect new risks, regulatory changes, or business growth.

10. Testing Scenarios

The test should be based on “worst case scenarios”. A comprehensive Work from Home (WFH) or Go Home (GH) plan may be invoked in (but not limited to) following disaster scenarios.

- Network Failure
- Power Outage
- Application Failover
- Communication Failure
- Personnel Unavailability
- Natural Disaster
- Cybersecurity Incident
- Physical Site Disaster
- Data Integrity
- Data Backup and Recovery failure
- External Service Provider Failure
- Business Partner Disruption
- Data Center Failure

The following factors should be considered while designing the BCP.

28. BCP DR Policy

- Probability of unplanned events, including natural or man-made disasters, earthquakes, fire, hurricanes or bio-chemical disaster
- Security threats
- Increasing infrastructure and application interdependencies
- Regulatory and compliance requirements, which are growing increasingly complex.
- Failure of key third party arrangements
- Globalization and the challenges of operating in multiple countries.

11. BCP / DR for IT Service Outsourcing

When engaging in IT service outsourcing, shall align its Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) with the requirements and guidelines set forth by regulatory bodies such as the Reserve Bank of India (RBI). Here's an outline of key considerations for BCP/DR for IT service outsourcing.

12. Policy Exception

Any exclusions to this policy shall be approved through the policy waiver.

Exceptions will not be universal but will be agreed on a case-by-case basis, upon official request made by the information owner. The waiver request must include, at a minimum, the following: Justification for the exception:

- Risk due to the exception
- The mitigation controls to manage the risk
- The plan of action to manage the risk
- The validity period of the exception and
- Details of assets on which the exception is applicable

13. Policy Compliance

- All the requirements specified in the Information Security Policy are to be followed by all employees of POLYCAB.
- Compliance to this policy will be measured by the internal or external audits.
- individual or a committee found to be not complying with the requirements specified in the policy is bound to accept consequences specified in Compliance Management Policy

14. Review and Update

This policy shall be reviewed annually and updated as necessary to reflect changes in process, technology, laws, or regulations.

15. Annexure

DR Procedure

28. BCP DR Policy



025 - Disaster
Recovery Procedure

DR Plan



DR Plan Temaplte

16. Control Reference

ISO 27001:2022

- Clause 6.1 | Actions to Address Risks and Opportunities
- Clause 6.1.3 | Information Security Risk Treatment
- Clause 8.1 | Operational Planning and Control
- Annex A 5.29 | Information Security During Disruption
- Annex A 5.30 | ICT Readiness for Business Continuity

Other policy and Procedure Cross Reference:

- Backup Policy
- Risk Management
- Capacity Management