POLYCAB

BCP DR Policy

Document Details

Title: 025 – BCP DR Policy	Document Owner: Cyber Security Team
Document Author(s): Sanket Mhatre	Version: V1.0
Classification: Polycab - Internal	Release Date: 10-04-2025

Version Details

Sr No.	Version	Date	Modified By	Reviewed By	Approved By	Comments
1	V1.0	04-Apr-25	Sanket Mhatre -IT Cyber Security (GRC)	Vijit Patil – CISO Ashish Anekar – IT Infra Head	Gandharv Tongia - CFO/CIO	Updated to align with industry standards (NIST and ISO 27001)

Contents

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. 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.

3. Scope

- 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.

4. Business Continuity Management Structure

4.1 DRBCP Committee

The DRBCP Committee comprises of CEO and Chief Information Officer The Committee is supported by Head Administration, Head —Digital, Head— HR. and Head - IT.

4.2 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.

4.3 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.
- 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.

4.4 During Disaster/Emergency (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.

4.5 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.

5. Business Continuity Strategy

- Business Continuity Planning

  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.

5.1 Risk Assessment

- The risk assessment conducted for POLYCAB involved a comprehensive analysis of potential risks across various domains to ensure the safety and well-being of employees, stakeholders, and the organization.
- The assessment encompassed hazards related to safety, health, environment, and security, considering both internal and external factors.
- Through a systematic process of hazard identification, risk analysis, and evaluation, we identified the likelihood and potential severity of risks, allowing us to prioritize and develop appropriate mitigation strategies.
- These strategies incorporated a hierarchy of controls, including elimination, substitution, engineering controls, administrative controls, and personal protective equipment, tailored to the specific needs and requirements of our organization.
- Implementation of the selected controls was meticulously coordinated, with clear responsibilities assigned and resources allocated accordingly. Ongoing monitoring and review mechanisms were established to ensure the effectiveness of the implemented controls and to promptly address any emerging risks or changes in circumstances.
- The risk assessment summary serves as a valuable reference for future assessments and enables us to maintain a proactive approach to risk management, fostering a safe and secure environment for all stakeholders involved.

5.2 Risk Assessment Objectives

- The primary objective of conducting a risk assessment within POLYCAB is to systematically identify, assess, and mitigate potential risks across all areas of operation. By undertaking this process, our organization aims to achieve the following specific objectives:
- Ensure Safety and Well-being: The foremost objective of the risk assessment is to safeguard the safety and well-being of our employees, customers, visitors, and any other individuals associated with our organization. By identifying hazards and evaluating risks, we can implement effective control measures to prevent accidents, injuries, and potential harm.
- The risk assessment helps protect our organization's valuable assets, including physical assets, intellectual property, and financial resources. By identifying vulnerabilities and potential threats, we can develop strategies to minimize the risk of theft, damage, or loss.
- It is also to ensure compliance with applicable laws, regulations, and standards. Through the risk assessment, we identify risks that may pose legal or regulatory liabilities and develop control measures to mitigate these risks, thereby avoiding penalties, fines, or reputational damage.
- The risk assessment enables us to identify risks that could disrupt our operations, such as natural disasters, technological failures, or supply chain disruptions. By proactively identifying and addressing these risks, we aim to minimize the potential for business interruptions and maintain continuity.
- A comprehensive risk assessment provides valuable insights into the potential risks associated with different activities, projects, or processes. These insights support informed decision-

making by enabling us to prioritize actions, allocate resources effectively, and determine risk tolerance levels.

- By conducting risk assessments regularly, we foster a culture of resilience within the organization. This includes building awareness, enhancing preparedness, and ensuring timely response and recovery in the face of potential risks or crises.
- Through a proactive and well-documented risk assessment process, we demonstrate our commitment to the safety and security of our stakeholders. This helps build trust, enhance reputation, and instil confidence among employees, customers, investors, and regulatory authorities.
- The risk assessment process is not static but dynamic, evolving with the changing organizational landscape. By continuously monitoring and reviewing the effectiveness of control measures and updating the risk assessment as necessary, we strive for continual improvement in risk management practices.

5.3 Risk Identification

- During the risk assessment process at POLYCAB, a crucial step involves identifying hazards and potential risks across various activities, processes, and projects. The objective is to comprehensively understand the potential sources of harm or adverse events that may pose a threat to individuals, assets, operations, and the environment. The following details outline the methodology and key considerations employed in hazard identification:
- We engage subject matter experts from relevant departments or fields to participate in brainstorming sessions. This collaborative approach allows for diverse perspectives, knowledge sharing, and the identification of hazards that might be overlooked by individual assessments.
- We analyse past incident reports, accidents, near-misses, and relevant data to identify recurring patterns or trends. Such reviews offer insights into potential hazards and risks associated with specific tasks, equipment, or work environments.
- Conducting site visits and actively observing work processes provides an opportunity to identify hazards firsthand. This on-site assessment helps in recognizing physical hazards, unsafe practices, inadequate safety measures, or environmental risks that may not be apparent from documentation alone.
- We review organizational policies, procedures, manuals, and relevant literature, including industry-specific guidelines and regulations. This step aids in identifying potential hazards and risks specific to our operations, aligning our assessment with established best practices and legal requirements.
- We involve stakeholders, including employees, contractors, and other individuals directly or indirectly impacted by our operations, to gather their insights and perspectives on potential hazards. Their input provides valuable information on risks that may have been overlooked by the internal assessment team.

5.4 Analyse And Evaluate Risks

- After assessing the identified risks during the risk assessment process at POLYCAB, the next crucial step is to analyse and evaluate those risks in more detail. This step involves a comprehensive examination of various factors related to the identified risks. The following details outline the methodology and key considerations employed in the analysis and evaluation of risks:

- To gain a deeper understanding of the identified risks, additional data may be collected. This can involve gathering information from relevant sources, conducting targeted studies or tests, consulting subject matter experts, or analysing incident reports and historical data. The purpose is to acquire more specific and detailed information about the risks, their potential causes, and their impacts.
- An analysis of risk frequency and duration helps in determining the likelihood and duration of exposure to the identified risks. This involves assessing the frequency at which the risk events can occur and the duration of time during which individuals or assets may be exposed to the risks. Understanding these factors aids in estimating the overall risk levels more accurately.
- Evaluating the potential exposure levels to the identified risks is essential for assessing their potential impacts. This analysis may involve measuring or estimating the extent of exposure to hazardous substances, physical hazards, or environmental factors. By considering factors such as concentration levels, proximity, duration, and potential pathways of exposure, a more comprehensive understanding of the risks is obtained.
- The evaluation of existing control measures or risk mitigation strategies is crucial in determining their effectiveness in managing or reducing the identified risks. This assessment involves reviewing the implemented controls, examining their compliance with applicable regulations and standards, and assessing their efficacy in minimizing or eliminating the risks. Any gaps or shortcomings in the existing controls are identified, and recommendations for improvements are made.
- The acceptability of risks is reevaluated based on the results of the detailed analysis and evaluation. This reassessment takes into account the refined understanding of the risks, their potential impacts, and the effectiveness of existing controls. Risks that were initially considered acceptable may be reclassified as unacceptable if their potential consequences or likelihood are found to be higher than previously estimated.
- Based on the analysis and evaluation of risks, appropriate risk treatment options are identified. This involves exploring various risk mitigation strategies and control measures that can effectively reduce the identified risks to acceptable levels. The risk treatment options may include implementing engineering controls, administrative controls, personal protective equipment, or other risk reduction measures based on the hierarchy of controls.
- A comprehensive record of the risk analysis and evaluation process is documented, including the detailed analysis findings, evaluation results, identified gaps or weaknesses, and recommended risk treatment options. This documentation provides a clear reference for decision-making, future risk assessments, and ongoing risk management efforts.
- By conducting a detailed analysis and evaluation of risks, Model gains a deeper understanding of the specific characteristics and potential impacts of the identified risks. This enables the organization to develop targeted and effective risk treatment strategies, enhance existing control measures, and prioritize resources to manage risks in a proactive and efficient manner. Regular monitoring and reassessment of risks ensure that risk management practices remain up-to-date and aligned with the evolving organizational needs and external factors.

5.5 Risk Mitigation

- Following the analysis and evaluation of risks during the risk assessment process at POLYCAB the next crucial step is to develop risk mitigation strategies. Risk mitigation aims to minimize or eliminate the identified risks and their potential impacts. The following details outline the methodology and key considerations employed in developing risk mitigation strategies:

- The risk mitigation strategies align with the hierarchy of controls, which prioritizes the most effective measures to control risks. The hierarchy includes elimination, substitution, engineering controls, and administrative controls. The strategies selected depend on the nature of the risks and the feasibility of implementing various control measures.
- The most effective approach is to eliminate the identified risks altogether whenever possible. This involves removing the hazard or substituting it with a safer alternative. If elimination or substitution is not feasible, efforts are made to minimize the risk through other control measures.
- Engineering controls involve modifying the physical environment or processes to reduce or eliminate the risk. This may include installing safety barriers, implementing ventilation systems, incorporating automated safety features, or redesigning workstations to minimize exposure to hazards. These controls focus on preventing the risk at its source.
- Administrative controls involve implementing policies, procedures, and protocols to manage risks. This can include developing clear safety guidelines, providing adequate training and education to employees, establishing effective communication channels, and implementing standardized work practices. Administrative controls aim to change behaviours and create a safety-conscious culture within the organization.
- Risk mitigation strategies are integrated into existing processes, procedures, and workflows. This ensures that the control measures become an integral part of day-to-day operations. The implementation of the strategies is coordinated across different departments or teams, with clear responsibilities assigned to relevant individuals or stakeholders.
- Adequate resources, including financial, human, and technological resources, are allocated to support the implementation of risk mitigation strategies. A budget is allocated to procure necessary equipment, conduct training programs, update infrastructure, or engage external expertise when required. Ensuring sufficient resources enhances the effectiveness of the risk mitigation efforts.
- Ongoing monitoring and periodic reviews are established to assess the effectiveness of the implemented risk mitigation strategies. This includes conducting regular inspections, audits, and evaluations to ensure compliance and identify areas for improvement. Any changes in the organizational context or emerging risks are promptly addressed through timely adjustments to the mitigation strategies.
- A comprehensive record of the developed risk mitigation strategies, including the rationale behind each strategy, implementation plans, and associated responsibilities, is documented. This documentation serves as a reference for stakeholders and helps maintain consistency and accountability in risk management practices.

5.6 Control Implementation

- Following the development of risk mitigation strategies, the next crucial step in the risk assessment process at POLYCAB is to implement controls. Controls are the specific measures and actions put in place to mitigate identified risks and reduce their potential impact. The following details outline the methodology and key considerations employed in implementing controls:
- Assigning clear roles and responsibilities is essential for effective implementation of controls. Designate individuals or teams responsible for implementing specific control measures, monitoring their effectiveness, and ensuring compliance with established protocols. This promotes accountability and ensures that control measures are appropriately executed.

- Effective communication is vital to ensure that all employees and stakeholders understand the implemented controls and their importance. Conduct comprehensive training programs to educate personnel on the purpose and proper execution of control measures. This includes providing guidance on using equipment, following protocols, and adhering to safe work practices.
- Implement engineering controls identified in the risk mitigation strategies. This may involve installing safety equipment, upgrading infrastructure, modifying workstations, or incorporating automation to reduce or eliminate risks. Ensure that engineering controls are properly designed, installed, and maintained to maximize their effectiveness.
- Enforce administrative controls through policies, protocols, and practices. This includes implementing safety protocols, establishing regular inspection schedules, conducting safety meetings, and enforcing compliance with established procedures. Regularly communicate safety expectations and reinforce a culture of safety throughout the organization.
- Regularly monitor the implementation of controls to assess their effectiveness. This can include conducting inspections, audits, or evaluations to ensure compliance with established procedures and identify any gaps or areas for improvement. Utilize technology, such as sensors or monitoring systems, where applicable, to enhance control monitoring capabilities.
- A robust incident reporting system shall be established to encourage employees to report near misses, accidents, or potential hazards. Investigate incidents promptly to identify root causes and determine whether control measures need adjustment or reinforcement. Use incident data to continually improve control implementation and address systemic issues. (Ref. Incident Management Policy and Procedure for the details)
- Foster a culture of continuous improvement by regularly reviewing and evaluating control effectiveness. Engage employees in providing feedback and suggestions for enhancing controls. Periodically reassess risks and adjust controls, accordingly, taking into account changes in processes, technologies, or external factors.
- Maintain thorough documentation of control implementation, including records of training sessions, inspections, audits, incident reports, and any changes or updates to control measures. Proper record-keeping ensures traceability, supports regulatory compliance, and facilitates ongoing monitoring and review of control effectiveness.

5.7 Monitoring And Reviewing

Monitoring and reviewing the effectiveness of risk management practices is a crucial aspect of the risk assessment process at POLYCAB. It ensures that identified risks are continuously monitored, control measures are functioning as intended, and any emerging risks or changes in the organizational context are promptly addressed. The following details outline the methodology and key considerations employed in monitoring and reviewing the risk assessment:

- Key performance indicators (KPIs) shall be established to monitor the effectiveness of risk management efforts. These KPIs should align with the goals and objectives of the organization and provide measurable metrics to track progress. Examples of KPIs include the number of incidents, near misses, compliance rates, training completion rates, and the effectiveness of control measures.
- Collect relevant data to assess the performance of risk management activities. This can include incident reports, inspection findings, audit results, employee feedback, and any other

data sources that provide insights into the effectiveness of implemented controls. Analyse the collected data to identify trends, patterns, or areas requiring improvement.

- Conduct regular inspections and audits to evaluate the implementation and effectiveness of control measures. This includes physical inspections of equipment, work areas, and processes to identify any deviations from established protocols. Audits help assess compliance with regulatory requirements, internal policies, and industry standards. Any non-compliance or deficiencies found during inspections or audits should be addressed promptly.
- Employees shall be encouraged to report incidents, near misses, or potential hazards through a robust reporting system. Investigate incidents to determine the root causes and identify any weaknesses in control measures. Use the findings from incident investigations to improve controls, update risk assessments, and prevent similar incidents from occurring in the future.
- Seek feedback from employees, supervisors, and other relevant stakeholders on the effectiveness of risk management practices. This can be done through surveys, focus groups, or regular communication channels. Gathering feedback helps identify areas for improvement, captures different perspectives, and fosters a culture of continuous improvement and open communication. Conduct regular management review meetings to discuss the performance of risk management activities. These meetings provide an opportunity to review the collected data, evaluate the effectiveness of controls, and make informed decisions regarding risk mitigation strategies. Management reviews ensure that risk management practices remain aligned with organizational goals, regulatory requirements, and industry best practices.
- Based on the findings from monitoring and reviews, identify areas for improvement and develop action plans. These initiatives may include updating control measures, providing additional training or resources, enhancing communication channels, or implementing new technologies. Continuously strive to enhance risk management practices and adapt to changing circumstances.
- Maintain comprehensive documentation of monitoring and review activities, including collected data, analysis results, action plans, and decisions made. Proper record-keeping ensures transparency, supports compliance efforts, and provides a historical reference for future risk assessments and management activities.

5.8 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).

5.9 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.

5.10 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.

6. Impact Rating

IMPACT RATING MATRIX -

Impact Scale					
Impact Categories	**1 - Incidental**	**2 - Minor**	**3 - Moderate**	**4 - Major**	**5 -Severe**
Financial	<=0.05% negative deviation in Net Profit.	>0.05% but <=0.1% negative deviation in Net Profit.	>0.1% but <=0.15% negative deviation in Net Profit.	>0.15% but <=0.25% negative deviation in Net Profit.	>0.25% negative deviation in Net Profit.
Regulatory	Isolated regulatory / compliance issues that are quickly remedied with little or no impact.	Routine regulatory finding that has low or no impact in terms of regulatory notice / fines.	Repeated regulatory findings. / Issues culminating into targeted regulatory scrutiny or investigation with regulatory censure and penalty / fines imposed.	Sustained scrutiny by regulatory body or bodies and/or significant fines and/or formal undertaking obtained by regulator from management	Sustained instances of non-compliance forcing regulatory bodies to Suspend the entity's license.

Reputational	No or Insignificant negative publicity and/or minor short-term damage – can be remedied quickly (through corrective measures) within few hours.	Limited adverse (Mainstream and social) media attention and/or some short-term damage and/or complaint to industry body – can be remedied (through corrective measures) within1-2 days.	Local adverse (mainstream and social) media attention and/or substantial short to medium term damage – though can be remedied (through corrective measures and may also requiring investment in PR) relatively slowly within 3 – 4 days.	Sustained local / national adverse (mainstream and social) media attention and/or Substantial medium to long term damage- requiring sufficient investment in PR besides aggressive action to remediate within 1 – 2 weeks.	Sustained regional / international adverse (mainstream and local) media attention and/or substantial long-term damage – requiring sustained investment in PR and remediation efforts.
Customer	Minimal impacts to part of customer base, channel, portfolio or region with < 1%	Impacts small part of customer base, channel or portfolio (>1% but < 2% customers impacted)	Impacts some part of customer base, channel or portfolio – (>2% but < 5% customers impacted)	Significant impact to most customers in one channel or region- (>5% but < 10% customers impacted)	Significant impact to most/all customer base, channel or portfolio (> 10% customers impacted)

	customers impacted				
Staff	Adverse impact to our people and limited to local. team or one team within one line of business / division.	Adverse impact to our people in more than one team within one line of business / Division.	Adverse impact to our people in more than one line of Business / Division	Loss of key specialist team(s) or significant impact to our People in more than one line of business / division.	Widespread escalations to labor ministry by former employees or adverse impact to most/all our people

7. BCP Scenarios and Management Plan

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

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

1. Primary site is not accessible, but primary data center and DR site are available.
   Trigger Event
   i. Epidemic/Pandemic
   ii. Non-Pandemic like riots, floods, war, geo-political issues, fire, structural damage, environmental contamination, etc. Response and recovery measures

1. Create awareness amongst the employees on various preventive measures to fight against the epidemic/ pandemic outbreak and/ or precautions to stay safe.
2. Necessary facility arrangements for sanitization shall be made at all the office locations and communicated to employees for the Epidemic / Pandemic scenario.
3. Information Technology team to access the IT infrastructure from the Corporate Office via Secure Connection
4. Identified critical personnel to resume critical processes through remote access to systems and applications which has been provided considering security & data protection. Employees shall access the IT facilities through Internet using secured authentication from their remote location.
5. Remote access to systems via secured channel to be provided to additional personnel which may include vendor staff and auditors as identified by the Departmental Heads and in line with the criticality of the processes.
6. Ster fumigation activity for office premises shall be carried out at regular activity in Epidemic/ Pandemic scenario when phase wise resumption to office is initiated.

7. Safety advisories to be followed while at office premises including social distancing, basic hygiene, etc. communicated by the HR team.

2. Primary site is accessible, but primary data Centre is disrupted Trigger Event

1. Any incident affecting the primary data Centre such as damage to equipment's and infrastructure, etc. Response and Recovery Measures
2. Any Incident should be reported to the concerned HOD member of committee.
3. IT team to provide the necessary communication to the employees giving the details of the incident, time required for resumption and any other instructions as required.
4. IT team to activate the DR site in line with defined IT Recovery procedures.
5. Resumption for the applications to be prioritized by the IT team based on process criticality.
6. Employees to resume working accordingly as per the instructions and arrangements made by the BU head & Application HOD
7. Employees of each department to prioritize the activities as per their individual SOPs prepared in case DRBCP is flagged off.

3. Primary site is accessible but both data center.

i.e. Primary and DR site is disrupted.

Trigger Event: Ransomware Response and Recovery Measures

Report the incident to the BU head & Application

1. Alert the employees and provide instructions w.r.t. disconnecting from the network.
2. Refer Cyber Crisis Management Plan for all the Ransomware related Incident response, containment and incident recovery and preventive measures.
3. IT team, Emergency team and / or the respective BCP coordinators from each team to provide the necessary communication to the employees given the details of the incident, time required for resumption and any other instructions as required.
4. Resumption from other media such as tapes to be initiated by the IT team based on process criticality as per
5. Employees to resume working accordingly as per the instructions and arrangements made by the BCP Coordinators and the Emergency Team
6. Employees of each department to prioritize the activities as per Annexure 1 and as defined in their individual SOPs prepared.
7. Employees shall assess and inform about any data loss to IT team for recovery and restoration.

4. Any Plant/branch office is inaccessible.

Trigger Event

- Loss of connectivity
- Any catastrophic event resulting in inaccessibility to one or multiple branches Response and Recovery Measures

1. Office Manager, Risk team, IT Team and Admin team
2. Check feasibility to conduct the business operations from other branches within the city wherever possible or from the nearest branch or Head office.
3. Remote access to systems to designated personnel to be provided considering security & data protection. Employee will access the IT facilities through Internet using secured authentication.

5. Cyber Incidents

Incident response, containment, recovery and preventive measures for various cyber crisis scenarios have been mentioned in detail in the Cyber Resilience Policy.

8. BCP Internal Audit

- POLYCAB shall ensure that internal audit of the BCP is conducted on a periodic basis (Cyber Security Team ownership) to determine whether the BCPS:
- Conforms to planned arrangements for BCP has been properly implemented and is maintained.
- Is effective in meeting the BCP policy and objectives as documented in the BCPS manual.
- Provide information on the results of the internal audits to the management.

9. Exceptions

All statutory, non-statutory and third-party employees must comply with the statements in this policy with immediate effect. Protection and support to be provided for all POLYCAB employees, assets and business in the event of disruption and ensure that critical activities continue in the event of the disaster.

Where a longer transition is required to achieve compliance, a documented business justification shall be submitted with proposed timelines (exceptional basis) to the BCP Steering Committee for approval.

Any exceptions to this policy shall be clearly documented and submitted to the BCP Steering Committee for evaluation and approval.

10. Continual Improvement

10.1 Management Review

Each Department shall conduct self-assessments periodically to ensure that the FRPs are relevant and up to date. The Steering Committee shall meet at least twice in a year to review the self-assessment and internal audit reports, and to provide approvals for changes, if required. The recommended time period for self-assessments tests is at least yearly once during BAU.

10.2 BCP Maintenance

BCP shall be continuously monitored to ensure that changes in Departments and supporting infrastructure are understood and reflected in the Business Continuity Strategy, procedures and plans. Improvements identified as a result of testing and training shall be included in the BCP as well as the annexures including documentation templates.

10.3 Nonconformity and Corrective Actions

POLYCAB shall take action to eliminate the cause of nonconformities identified with the implementation and operation of the BCP to prevent their recurrence. All such action taken shall be documented and presented to the Steering Committee.

11. Dependency Analysis

Analysing dependencies is a crucial step in developing a comprehensive Business Continuity Plan (BCP) at POLYCAB. It involves identifying and understanding the interdependencies between various systems,

processes, resources, and stakeholders within the organization. By analysing dependencies, the organization can assess potential vulnerabilities, determine critical dependencies, and develop effective strategies for maintaining continuity in the event of a disruptive incident. The following details outline the methodology, and key considerations shall be involved in analysing dependencies for BCP:

11.1 Identify Dependencies:

- Identify the organization's critical systems, including IT infrastructure, networks, servers, databases, and applications. Determine their interdependencies and relationships.
- Analyse the organization's core processes, workflows, and procedures. Identify dependencies between different departments, teams, and individuals involved in the execution of these processes.
- Identify critical resources and suppliers that the organization relies on for its operations. Determine the dependencies on external parties for the supply of goods, services, or expertise.
- Consider dependencies on internal and external stakeholders, such as customers, regulatory bodies, partners, and vendors. Assess the impact of their actions or inactions on the organization's operations.

11.2 Dependency Mapping:

- Create dependency maps or diagrams that illustrate the relationships between systems, processes, resources, and stakeholders. This visualization helps identify complex dependencies and understand the potential ripple effects of disruptions.
- Engage relevant stakeholders, subject matter experts, and department heads to gather information about dependencies. Conduct interviews, workshops, or surveys to gain insights into the interconnectedness of different components within the organization.
- Document the identified dependencies, including their nature, direction, and criticality. Maintain an updated repository or database of dependencies for reference during BCP development and incident response.

11.3 Mitigation Strategies:

- Develop alternative strategies or workarounds for critical dependencies. Identify backup systems, redundant resources, alternative suppliers, or alternative processes that can be activated in the event of a disruption.
- Establish effective supplier management practices, including contingency plans, service level agreements, and regular communication with key suppliers. Ensure that suppliers also have their own BCPs in place to address potential disruptions.
- Analyse processes and workflows to identify opportunities for reducing dependencies or creating more resilient systems. Consider automation, decentralization, or reengineering of processes to minimize reliance on specific dependencies.
- Promote cross-training and knowledge sharing among employees to reduce dependency on specific individuals or skill sets. Ensure that critical knowledge is documented and accessible to relevant stakeholders.

11.4 Testing and Validation:

- Conduct scenario-based tests or simulations to validate the effectiveness of the BCP's dependency mitigation strategies. Create test scenarios that simulate various dependency

failures and assess the organization's ability to respond, recover, and maintain critical operations.

- Organize tabletop exercises involving key stakeholders to simulate real-world scenarios and evaluate the organization's response to dependency disruptions. These exercises help identify gaps, refine response procedures, and improve coordination among teams.
- Perform technical testing to assess the resilience of critical systems and infrastructure. This may include conducting penetration testing, vulnerability assessments, and disaster recovery drills to validate the organization's ability to restore dependencies within the required timeframes.
- Communication and Coordination Testing: Evaluate the effectiveness of communication and coordination mechanisms during dependency disruptions. Test the organization's ability to communicate with internal and external stakeholders, activate alternative dependencies, and coordinate response efforts.
- Capture lessons learned from testing and exercises and use them to refine the BCP. Identify areas of improvement, update dependency maps and documentation, and implement corrective actions to address vulnerabilities or weaknesses.

11.5 Continuous Review and Monitoring:

- Continuously monitor and assess dependencies within the organization to identify changes or emerging risks. Regularly review the dependency maps, update them as needed, and reassess the criticality and impact of dependencies.
- Establish robust change management processes to ensure that any changes in systems, processes, resources, or suppliers are thoroughly evaluated for their potential impact on dependencies. Assess the need for adjustments or updates to the BCP based on these changes. (Ref. the Change Management Policy for the details)
- Stay informed about external factors that may affect dependencies, such as industry trends, regulatory changes, or technological advancements. Monitor the performance and resilience of external suppliers or service providers and maintain open lines of communication with them.

11.6 Mitigation Strategies

Developing effective mitigation strategies is a critical component of a robust Business Continuity Plan (BCP) at POLYCAB. Mitigation strategies aim to minimize the impact of disruptive incidents and ensure the organization can continue its critical functions. The following details outline the methodology, and key considerations shall be involved in developing mitigation strategies for BCP:

- Based on the identified risks and their potential impacts, explore various mitigation options. These may include preventive measures, redundant systems, backup solutions, insurance coverage, alternate suppliers, or diversification of resources.
- Consider transferring certain risks to third parties through insurance policies or service level agreements. This helps mitigate financial losses and provides support in case of disruptions.
- Evaluate critical business processes to identify opportunities for streamlining, automation, or redundancy. Redesign processes to reduce single points of failure and enhance resilience.
- Introduce redundancy in critical systems and infrastructure to mitigate the impact of failures or disruptions. This can involve duplicating hardware, establishing backup servers, or implementing failover mechanisms.

- Regularly back up critical data and systems to ensure quick recovery and minimize data loss in the event of a disruptive incident. Test and validate the effectiveness of backup systems and data restoration procedures.
- Identify alternative work procedures and locations to ensure business continuity during disruptions. This can involve establishing remote work capabilities, identifying backup facilities, or implementing flexible work arrangements.
- Document and communicate the alternative work procedures to relevant employees, ensuring they understand their roles and responsibilities in executing these procedures.
- Strengthen cybersecurity measures to protect critical systems and data from cyber threats. This can involve implementing robust firewalls, intrusion detection systems, data encryption, and user access controls.
- Conduct regular cybersecurity audits and vulnerability assessments to identify and address potential weaknesses in the organization's IT infrastructure. Conduct regular tests, drills, and tabletop exercises to validate the effectiveness of mitigation strategies. This helps identify gaps, weaknesses, and areas for improvement in the BCP.
- Continually review and update mitigation strategies based on lessons learned from testing, real incidents, changes in dependencies, or advancements in technology.

11.7 Cost-Benefit Analysis (Cba)

Cost-Benefit Analysis (CBA) is a valuable tool that assesses the financial implications and potential benefits of implementing and maintaining a robust Business Continuity Plan (BCP) at POLYCAB. CBA enables organizations to make informed decisions by comparing the costs of implementing BCP measures against the expected benefits and value derived from risk mitigation and ensuring uninterrupted business operations.

The following details outline the methodology and key considerations involved in conducting a comprehensive cost-benefit analysis for the BCP:

Identify Costs:

- Identify the initial costs required to develop and implement the BCP. This includes expenses associated with risk assessment, business impact analysis, consulting services, software, hardware, training, and any necessary infrastructure upgrades.
- Determine the recurring costs involved in maintaining and updating the BCP. This can include costs for regular testing and exercises, employee training, system maintenance, backup systems, and periodic review and updates of the plan.

11.8 Quantify Benefits:

- Assess the potential reduction in financial losses and operational disruptions that can be achieved through effective BCP implementation. Consider the potential costs associated with disruption, such as revenue loss, customer dissatisfaction, regulatory penalties, legal liabilities, reputation damage, and recovery expenses.
- Quantify the value derived from minimizing downtime, reducing the time taken to recover critical functions, and maintaining operational continuity during disruptive incidents. Consider the potential benefits of improved customer trust, increased market competitiveness, and the ability to fulfil contractual obligations.
- Evaluate the positive impact on stakeholder confidence, including customers, suppliers, investors, and regulatory bodies. Consider the potential benefits of maintaining strong

relationships, meeting compliance requirements, and demonstrating a commitment to operational resilience.

11.9 Evaluate Tangible and Intangible Factors:

- Consider measurable and quantifiable factors such as direct financial savings, revenue protection, cost avoidance, and reduced recovery expenses.
- Assess the value of intangible benefits that may be challenging to quantify, such as brand reputation, customer loyalty, employee morale, and regulatory compliance.

11.10 Assign Monetary Values:

- Assign monetary values to both the costs and benefits identified in the analysis. This may involve estimating potential losses and gains based on historical data, industry benchmarks, expert opinions, or past incidents.
- Apply appropriate discount rates to account for the time value of money when comparing present costs against future benefits.

11.11 Calculate the Net Present Value (NPV) And Return on Investment (ROI):

- Determine the NPV by subtracting the present value of the costs from the present value of the benefits. The NPV provides an estimate of the net financial value generated by the BCP over a specified time period.
- Calculate the ROI by dividing the NPV by the total investment costs and expressing it as a percentage. The ROI provides an indication of the financial efficiency and profitability of the BCP investment.

11.12 Sensitivity Analysis:

- Conduct sensitivity analysis to evaluate the impact of changing assumptions and variables on the cost-benefit outcomes. This helps identify key drivers and assess the robustness of the analysis.

11.3 Decision-Making and Prioritization:

- Consider the cost-benefit outcomes alongside other strategic considerations, risk appetite, and organizational priorities. Use the analysis as a basis for decision-making, resource allocation, and prioritizing BCP measures.

11.4 Review and Update:

- Regularly review and update the cost-benefit analysis as new information, technological advancements, or changes in the organizational context emerge. This ensures that the BCP remains aligned with evolving business needs and provides optimal value.

12. Business Impact Assessment (BIA)

Business Impact Assessment is to analyse the potential consequences of disruptive incidents on POLYCAB's operations, financials, reputation, and customer satisfaction. By conducting a thorough assessment, POLYCAB can identify its critical processes, resources, dependencies, and vulnerabilities. The BIA provides valuable insights to prioritize recovery efforts, allocate resources effectively, and develop a robust BCP and DR policy that aligns with the organization's overall strategic goals.

The following details outline the methodology and key considerations involved in conducting Business Impact Assessment (BIA) at POLYCAB

12.1 Identify Critical Business Functions

- The identification of critical business functions is a crucial step in developing a robust Business Continuity Plan (BCP) at POLYCAB. Critical business functions are the core activities that must be maintained or quickly restored during a disruptive event to ensure the organization's continuity. The following details outline the methodology, and key considerations shall be involved in identifying critical business functions:
- Engage key stakeholders, including department heads, managers, and subject matter experts, to gather their input on the organization's critical business functions. These stakeholders possess in-depth knowledge of the organization's operations and can provide valuable insights on the functions that are essential for its continued operation.
- Conduct a comprehensive business process mapping exercise to understand the end-to-end workflows and dependencies within the organization. This exercise involves documenting the various processes, sub-processes, inputs, outputs, and stakeholders involved in each business function. Mapping out the organization's processes helps identify the interdependencies between different functions and the potential impact of their disruption.
- Perform an impact analysis to assess the consequences of disruptions to different business functions. Consider both internal and external impacts, such as financial losses, operational downtime, regulatory compliance, reputation damage, and customer satisfaction. Evaluate the potential severity and urgency of these impacts to prioritize the recovery efforts.
- Determine the time sensitivity of each business function by evaluating the maximum tolerable downtime. This is commonly referred to as the Recovery Time Objective (RTO) and represents the acceptable duration within which a function must be restored to avoid severe consequences. Functions with shorter RTOs are typically considered more critical and require immediate attention during a disruptive event.
- Consider legal and regulatory obligations that may influence the criticality of certain business functions. Some functions may be critical due to compliance requirements or the need to meet specific industry standards. Identify functions that, if disrupted, could result in legal or regulatory non-compliance and prioritize their recovery accordingly.
- Assess the impact of each business function's disruption on customers, stakeholders, and the overall reputation of the organization. Functions that directly impact customer service, product delivery, or stakeholder relationships may be considered critical due to their direct influence on the organization's revenue generation and long-term sustainability.
- Evaluate the financial implications of the disruption of different business functions. Consider revenue loss, additional expenses, and the potential impact on profitability. Functions that have a significant financial impact or contribute to the organization's core revenue streams are often deemed critical.
- Identify dependencies between different business functions and assess the potential cascading effects of their disruption. Functions that serve as dependencies for other critical functions or have a widespread impact on multiple areas of the organization may be considered critical due to their ripple effects.
- Seek input from senior management to understand their perspective on critical business functions and their risk appetite. Management's insights can help align the identification of critical functions with the organization's strategic goals, priorities, and overall risk management approach.

- Document the identified critical business functions, their interdependencies, and the rationale behind their classification. Validate the identified critical functions with stakeholders to ensure their accuracy and consensus.

12.2 Risk Analysis

- Risk analysis is a vital component of developing a robust Business Continuity Plan (BCP) at POLYCAB. It involves systematically assessing potential risks and their potential impact on the organization's operations, enabling the identification of effective mitigation strategies. The following details outline the methodology, and key considerations shall be involved in conducting risk analysis for BCP:
- Begin by identifying a comprehensive list of potential risks that could disrupt the organization's operations. These risks may include natural disasters, technological failures, cyber-attacks, pandemics, supply chain disruptions, regulatory changes, and human-related incidents. Engage stakeholders, including subject matter experts, department heads, and risk management personnel, to gather their insights and expertise in identifying risks specific to the organization.
- Evaluate the likelihood and potential impact of each identified risk. Assess the probability of the risk occurring and the severity of its impact on the organization's critical functions, infrastructure, reputation, and financials. This assessment can be performed using qualitative or quantitative methods, depending on the organization's risk management practices and available data.
- Conduct a detailed Business Impact Analysis (BIA) to determine the potential consequences of various risks on the organization's critical functions, resources, and stakeholders. Assess the financial, operational, reputational, legal, and regulatory impacts that could arise from the occurrence of each risk. This analysis helps prioritize risks based on their potential severity and urgency for mitigation.

- Prioritize risks based on their likelihood and impact, considering the organization's risk appetite and business objectives. Focus on risks that have a higher likelihood of occurrence and those that would result in severe consequences if they were to materialize. This prioritization ensures that limited resources are allocated effectively to address the most significant risks.

- Identify vulnerabilities within the organization that could exacerbate the impact of certain risks. Assess the weaknesses in the organization's infrastructure, systems, processes, and human resources that could make it more susceptible to the identified risks. This assessment helps identify areas where targeted mitigation measures are needed to reduce vulnerabilities and enhance the organization's resilience.
- Develop control measures and mitigation strategies for each prioritized risk. These measures can include implementing preventive controls, such as redundancy in critical systems, conducting regular backups, implementing cybersecurity protocols, training employees on emergency response procedures, and establishing alternative communication channels. Determine the feasibility, effectiveness, and cost implications of each measure to ensure practical implementation.
- Develop recovery strategies that outline the steps to be taken to restore critical functions and minimize the impact of disruptions. This may include establishing alternative work locations, securing backup power sources, implementing data recovery procedures, and establishing communication protocols during emergencies. Ensure that recovery strategies align with the organization's Recovery Time Objectives (RTOs) established in the BIA.

- Establish a process for monitoring and reviewing risks on an ongoing basis. Regularly reassess the identified risks, their likelihood, and potential impact based on changes in the organization's environment, emerging threats, and evolving technology. Update mitigation strategies and recovery plans as needed to ensure their continued effectiveness.
- Document the risk analysis process, including the identified risks, their assessment, prioritization, control measures, mitigation strategies, and recovery plans. Communicate the outcomes of the risk analysis to key stakeholders, including senior management, employees, and relevant external partners, to ensure shared understanding and support for the BCP.
- Periodically test the effectiveness of the BCP through simulations, tabletop exercises, or full-scale drills. These tests help validate the mitigation measures, identify any gaps or areas for

12.3 Impact Evaluation

- Impact evaluation is a critical step in the development and maintenance of a robust Business Continuity Plan (BCP) at POLYCAB. It involves assessing the potential impact of disruptive incidents on the organization's operations, processes, stakeholders, and overall resilience. The following details outline the methodology, and key considerations shall be involved in conducting impact evaluation for BCP:
- Begin by identifying a range of potential scenarios or incidents that could disrupt the organization's operations. These scenarios may include natural disasters, technological failures, cyber-attacks, pandemics, supply chain disruptions, or any other events specific to the organization's industry or geographical location. Consider both internal and external factors that could lead to such incidents.
- Conduct a comprehensive Business Impact Analysis (BIA) to assess the consequences of the identified scenarios on the organization's critical functions, resources, and stakeholders. Evaluate the financial, operational, reputational, legal, and regulatory impacts that could arise from each scenario. This analysis helps quantify the potential severity and urgency of each scenario's impact.
- Establish Recovery Time Objectives (RTOs) for critical functions, representing the maximum tolerable downtime acceptable to the organization. RTOs help determine the timeframe within which each critical function should be restored to minimize the impact of disruptions. Align the RTOs with the organization's risk appetite, operational needs, and regulatory requirements.
- Assess the potential financial implications of each scenario on the organization. This includes estimating revenue losses, increased expenses, potential damage to assets, and the overall impact on profitability. Quantifying the financial impact helps prioritize resources and investments for mitigating and recovering from the identified incidents.
- Evaluate the operational impact of each scenario on the organization's processes, systems, supply chain, and workforce. Identify potential bottlenecks, vulnerabilities, and dependencies that could affect the organization's ability to deliver products or services. Analyse the potential disruptions to production, distribution, customer service, and other critical operations.
- Assess the impact of each scenario on the organization's stakeholders, including customers, employees, suppliers, and regulatory bodies. Consider the potential consequences on customer satisfaction, brand reputation, employee morale, and regulatory compliance. Identify key stakeholders and their specific concerns to develop targeted mitigation strategies and communication plans.

- Evaluate the impact of each scenario on the organization's compliance with relevant laws, regulations, and industry standards. Consider potential consequences related to data protection, privacy, safety, and security. Ensure that the BCP aligns with applicable legal and regulatory requirements and that recovery strategies consider compliance obligations.
- Assess the potential impact of disruptive incidents on the organization's supply chain. Identify critical suppliers, dependencies, and alternate sourcing options. Analyse potential disruptions to the flow of goods, services, and information within the supply chain. Develop strategies to mitigate risks and maintain continuity in the supply chain.
- Based on the impact evaluation, develop recovery strategies and plans to address each identified scenario. These strategies should include specific actions, responsibilities, and timelines for restoring critical functions and mitigating the impact of disruptions. Ensure that recovery strategies align with the organization's RTOs and prioritize resources accordingly.
- Regularly review and update the impact evaluation as new information becomes available or the organizational context changes. Monitor emerging risks, technological advancements, and regulatory updates to ensure the BCP remains effective and aligned with evolving circumstances. Conduct post-incident evaluations to identify lessons learned and improve the impact evaluation process for future incidents.

DETERMINING RECOVERY TIME OBJECTIVES (RTO) AND RECOVERY POINT OBJECTIVES (RPO):

Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are essential elements in developing an effective Business Continuity Plan (BCP) at POLYCAB. They provide guidance on the desired timeframe for restoring critical functions and the acceptable amount of data loss in the event of a disruptive incident. The following details outline the methodology and key considerations involved in determining RTO and RPO for BCP:

12.4 Recovery Time Objectives (RTO):

- Identify the organization's critical functions that are vital for its operations and would significantly impact its stakeholders if disrupted.

- Engage key stakeholders, including department heads, managers, and subject matter experts, to understand their requirements and expectations regarding the recovery time frame.
- Consider the time-sensitivity of each critical function. Determine the maximum tolerable downtime for each function, taking into account factors such as customer expectations, contractual obligations, regulatory requirements, and financial implications.
- Prioritize critical functions based on their impact and urgency for recovery. Functions with shorter RTOs, indicating a need for quick restoration, should be given higher priority in resource allocation and recovery planning.

RTO for Critical Process is ≤ 24 Hours, RTO for Non-Critical Process is > 24 Hours.

12.4 Recovery Point Objectives (RPO):

- Assess the organization's data landscape, including the volume, types, and criticality of data. Determine the data sources, repositories, and systems that support critical functions and must be restored during a disruptive incident.
- Determine the acceptable amount of data loss in the event of a disruption. This is often measured in terms of time, representing the maximum permissible time gap between the last available backup or recovery point and the incident occurrence.

- Consider the impact of data loss on the organization's operations, decision-making, customer service, compliance, and legal obligations. Consult with relevant stakeholders to understand their data requirements and the implications of potential data loss.
- Evaluate the capabilities of the organization's technology infrastructure, including backup systems, data replication mechanisms, and recovery mechanisms. Assess the feasibility and effectiveness of different data recovery strategies and technologies.
- Align the RPO with the organization's recovery strategies and technological capabilities. Determine the frequency of data backups, replication intervals, and recovery mechanisms to ensure that the RPO is achievable and aligns with the organization's risk tolerance and operational needs.

No	Applications / Asset	Departmentcriticality rating	Application / Asset CriticalityRating	RTO (Min)	RPO (Min)
1	Critical Applications	Critical	critical	30	**10**
2	Other supportingApplications	Important	Important	8 Hours	**30 minutes**

12.5 Real-Time RPO:

Many critical functions, have real-time data replication to ensure minimal data loss at POLYCAB. These functions RPO is set to minimal (zero), meaning that no data loss is acceptable. Continuous data replication mechanisms are implemented to mirror data in real-time across multiple geographically dispersed locations. This ensures that the latest transactions and customer data are always available and can be recovered immediately in the event of a disruption.

12.6 Near Real-Time RPO:

For other functions, such as Payment systems, IT Systems, a near real-time RPO is employed at POLYCAB. These functions are set to near real-time RPO is typically measured in Minutes or Couple of Hours. Data is replicated frequently to secondary sites or backup systems, ensuring that in the event of a disruption, minimal data loss occurs. This ensures that functions operations can be restored promptly with limited impact on customers and financial stability.

12.7 RTO & RPO For Applications

13. Recovery Strategies/Contingency Plan

POLYCAB shall develop appropriate recovery strategies focusing on the recovery of the critical business processes identified in BIA. On the basis of the results of the BIA, every department shall select a strategy or combination of the strategies (e.g.: teleworking, data backup, fallback sites, replacement solutions for applications etc.) in order to ensure the critical processes are resumed within their respective RTOs at an agreed service level.

Based on the above information captured, each department shall prepare a Functional Recovery Plan (FRP) mentioning the critical and vital business processes for each department along with the strategies implemented for each process.

13.1 Remote Access

- (Work from Home Strategy) - Critical business processes of respective departments from home by using Remote Access using POLYCAB provided Laptops.
- Identified key resources must be provided with internet access (Data card / Wi-Fi), Virtual Private Network (VPN) access and laptops to carry out their critical tasks.

13.2 Alternate Site/Backup Site Strategy

- 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 location(Head Office) is not accessible / available, the alternate site can be used as an alternate location to continue the operating business.

13.3 Displacement Strategy (Split Site Strategy)

- In this strategy the workload of the department during normal operations is divided and the activities are carried out from two or more cities. 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.
- Basis BIA Exercise conducted, following BCP strategies may be considered –

13.4 Incident Reporting and Crisis Communication

The Incident Management Plan (IMP) aims at establishing a formal structure with management representation, key roles & responsibilities, assignments to handle an event / incident / crisis, effectively communicating during and after the event / incident / crisis. It shall provide a framework within which decisions can be taken promptly during an emergency and ensure to:

- Save and protect the lives of people who are present in POLYCAB's premises.
- Continue providing critical services to its employees, consultants, contractors, vendor staff and other people present in POLYCAB's premises.
- Communicate effectively to all stakeholders on the situation.
- Manage resources effectively during and after the emergency.
- Contain loss and damage to property.
- POLYCAB shall develop and maintain plans that detail how incidents are to be managed. The IMP shall contain disaster preparedness checklist, details of command center, evacuation plan, call tree details and disaster management team details. Disaster Management teams shall be formed at each premise.

13.5 Business Continuity Principles

The following key principles may be followed for building an effective BCP DRP:

- Develop and practice a contingency plan that includes a succession plan for the Co. team.

- Determine offsite crisis meeting places and crisis communication for top executives. Practice crisis communication with employees, customers, and the outside world.
- Train backup employees to perform emergency tasks. The employees we count on to lead in an emergency may not always be available.
- Invest in an alternate means of communication in case the phone networks go down.
- Make sure that all employees as well as executives are involved in the exercises so that they get practice in responding to an emergency.
- Make Business Continuity exercises realistic enough to tap into employee's emotions so that their reactions can be observed when the situation gets stressful.
- Form partnerships with local emergency response groups e.g. firefighters, police, and local agencies to establish a good working relationship. Let them become familiar with the company and site.
- Evaluate company's performance during each test, and work toward constant improvement. Continuity exercises should reveal weaknesses.
- Test the continuity plan regularly to reveal and accommodate changes.

13.6 New Business Process and Systems

POLYCAB shall ensure that BCP considerations are considered during the planning stages for all new business processes and systems.

13.7 Business Continuity Exercise

- BCP shall be exercised at least once a year, and modifications shall be made wherever necessary to consider the exercise including joint testing with service providers/ vendors. BCP exercises shall be approved from relevant business teams, IT/ network team along with BCP Steering Committee (hereafter referred to as "Steering Committee" or "Committee"). The BCP exercise shall be documented and learnings from them shall be incorporated in the existing BCP.
- BCP Exercises include Desk Check or walkthrough of BCP, Tabletop Exercise, Call Tree Exercise, Full Simulation Exercise, etc. POLYCAB shall consider conducting either one, or a combination of two of the aforementioned exercises. The Steering Committee shall present a BCP Plan Exercise report to the Board of POLYCAB.

13.8 Business Continuity Planning and Testing

POLYCAB shall develop a business continuity plan and conduct business continuity test exercises. It will validate a range of severe but plausible scenarios that incorporate disruptive events and incidents; in order to check the ability to deliver critical operations through disruption. During Business as Usual (BAU)The testing shall be conducted at least twice in a year by each department and report submitted to BC Manager for Scrutiny (However testing exercise will not be conducted when Business Continuity Plan is in force).

The BC plan shall identify key internal and external dependencies to assess the risks and potential impact of various disruption scenarios on operations and ensure appropriate resilience levels. DBCCs are entrusted to develop the Plans in discussion with the BC manager and HODs. The plan shall incorporate the following-

- Business impact analysis
- Recovery strategies

- Escalation matrix
- Business continuity testing programs.
- Training and awareness programs
- Communication
- Crisis management programs

13.9 Testing Exercise Preparation

Each department will maintain the basic background data at all times in a year as a gesture of readiness. These will be detailed for each department for periodic testing and recorded by presenting the results to the BCP Steering Committee. DBCCs will be responsible for managing the comprehensive data in a MS word document format for ready reference. Indicative data points to be maintained by all departments for conducting a BIA and developing a BCP are stipulated below-

Complete department team staff details (employee code, name, unit, HOD, CxO, personal and official e-mail, personal Mobile, emergency contact, Communication & permanent address, age, sex, Asset requirements, System / Software used etc.)

- Department Hierarchy and reporting along with call tree details.
- List of Systems / software and their access controls and maintenance contact points.
- Physical Infrastructure requirement details for the team (Computers, desks, software, etc.) Team Capacity plan.
- List of Third-party vendors with complete details (employee strength, contact details, activity performed, BCP, etc.)
- Everyday vital data requirement details for BAU activity.
- List of critical and non-critical activities performed by the team. Establish a business process task breakdown of what is a critical activity, a postponed activity, and a best effort activity.
- Document the acceptable downtime for each critical function & system and create a plan to maintain operations. Define the RTO, RPO and in collaboration with the IT department constitute a detailed DR plan for each process and system in the department.
- Delegation of authority and dependencies on other departments
- Conduct emergency evacuation procedures and mock drill training and maintain the record of all such activities carried out for the department or Organization as a whole.
- Confidential data storage point and applicable DR site and revocation procedure
- Premises physical security maintenance checks.
- Unit key person succession plan.
- Copies of process guidelines, SOPs, DOIs, policy, Risk assessments etc.
- List of regulatory returns being filed.
- List of WIP and pending jobs.
- Details of pending legal proceedings if any.
- Train the staff on BCP and assign a BCP coordinator for the department.
- Fill the BIA format and keep ready for testing.
- Preparation of BIA on virtual scenarios.

13.10 Testing Frequency

The BC testing exercise shall comprise department wise once in a year and check of the above 21 data points by the Department / Business Unit Heads for readiness, accuracy and developing BIA & BC Plan.

13.11 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.

- 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.

13.12 BCP / DR for It Service Outsourcing

When engaging in IT service outsourcing, POLYCAB 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.

13.13 BCP and DRP Framework

A robust Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) framework is crucial when engaging in IT service outsourcing. It ensures that organizations are well-prepared to address disruptions and maintain business continuity. Here are the key components that shall be considered for a robust BCP and DRP framework for IT service outsourcing:

- Include specific contractual requirements related to BCP and DRP in the outsourcing agreement. Clearly define the service provider's responsibilities for developing, implementing, and maintaining their own BCP and DRP. Specify compliance with industry standards, regulatory requirements, and best practices.
- Conduct a comprehensive risk assessment and due diligence of the service provider's capabilities. Assess their BCP and DRP documentation, procedures, and track record. Evaluate their infrastructure, redundancy measures, data protection protocols, and business continuity capabilities. Ensure they align with your organization's risk tolerance and requirements.

- Ensure the service provider's BCP and DRP align with your organization's BCP and DRP. Verify that their recovery time objectives (RTOs) and recovery point objectives (RPOs) meet your business needs. Align the recovery strategies, communication protocols, and crisis management processes with your organization's standards.
- Establish clear communication channels and escalation procedures between your organization and the service provider during a disruption. Define communication protocols for incident reporting, progress updates, and resolution status. Ensure that lines of communication are readily available and accessible to all relevant stakeholders.
- Define data backup requirements and verify that the service provider has robust backup procedures and mechanisms in place. Ensure the regular and secure backup of critical data and applications. Validate the effectiveness of their backup and recovery processes through periodic testing and verification.
- Assess the availability of alternative service providers in case of a disruption or termination of the outsourcing agreement. Maintain a list of backup providers and evaluate their readiness to take over services if required. Define the criteria for transitioning services to an alternative provider, including data migration, knowledge transfer, and service-level agreements (SLAs).
- Regularly test the BCP and DRP of the service provider through drills, simulations, or tabletop exercises. Evaluate their preparedness, response capabilities, and ability to meet recovery objectives. Verify the effectiveness of their communication protocols, data restoration processes, and coordination with your organization.
- Periodically review the service provider's BCP and DRP documentation to ensure it remains up to date and aligned with changing requirements. Monitor their compliance with contractual obligations related to BCP and DRP. Conduct audits and assessments to verify their adherence to industry standards, regulations, and best practices.
- Encourage a culture of continuous improvement by promoting feedback and lessons learned from incidents, tests, and real-life scenarios. Identify areas for enhancement in the BCP and DRP framework. Collaborate with the service provider to implement corrective actions, update procedures, and incorporate best practices.
- Maintain comprehensive documentation of the outsourcing arrangement, including the BCP and DRP requirements. Provide training to relevant personnel within both organizations on their roles and responsibilities during a disruption. Ensure that employees are aware of the service provider's BCP and DRP procedures and know how to engage with them effectively.

13.14 Contingency Plan

- Contingency planning is a critical aspect of IT service outsourcing to ensure preparedness for potential disruptions and minimize the impact on business operations. The following key points shall be considered for effective contingency planning in IT service outsourcing:
- Identify the critical services and functions that are being outsourced. Understand their dependencies, interrelationships, and the potential impact of their disruption on the overall business operations. Prioritize the services and functions based on their criticality and determine the level of contingency planning required for each.
- Evaluate the availability of alternative service providers in case of a disruption or termination of the outsourcing agreement. Conduct due diligence on potential backup providers and assess their capabilities, expertise, and track record. Establish relationships and agreements with backup providers to ensure a smooth transition of services if needed.
- Include exit strategies in the outsourcing agreement that outline the process for transitioning services back in-house or to another service provider in case of a disruption. Define the terms,

timelines, and responsibilities for an orderly termination of the agreement. Ensure that the agreement includes provisions for the transfer of data, knowledge, and intellectual property rights.

- Require the service provider to have robust data backup and recovery mechanisms in place. Define the frequency, integrity, and retention period for data backups. Ensure that backup systems are regularly tested and that the restoration procedures are well-documented and understood by both parties. Consider off-site or cloud-based backup solutions for added resilience.
- Evaluate the service provider's infrastructure and ensure they have redundancy measures in place to minimize the impact of disruptions. Assess their scalability to handle increased demand or sudden surges in service requirements. Define the expectations and requirements for redundancy and scalability in the outsourcing agreement.
- Establish clear communication channels and escalation procedures between your organization and the service provider during a disruption. Define the points of contact, reporting mechanisms, and communication protocols. Ensure that all relevant stakeholders are aware of these channels and have access to them in case of emergencies.
- Regularly test and exercise the contingency plans with the service provider. Conduct tabletop exercises or simulations to validate the effectiveness of the plans and identify areas for improvement. Test the communication channels, data restoration processes, and coordination between your organization and the service provider during these exercises.
- Continuously monitor the performance of the service provider and assess their compliance with the agreed-upon contingency plans. Conduct periodic reviews and audits to ensure that the plans remain up to date and aligned with changing requirements. Incorporate lessons learned from real incidents or exercises to enhance the effectiveness of the contingency plans.
- Educate and train employees within your organization about the contingency plans and their roles and responsibilities during a disruption. Ensure that employees understand how to engage with the service provider and follow the established communication protocols. Regularly communicate updates and changes to the contingency plans to keep employees informed.
- Maintain comprehensive documentation of the contingency plans, including procedures, contact lists, and recovery strategies. Ensure that this documentation is easily accessible to all relevant stakeholders, including employees and key decision-makers. Store the documentation securely and have backup copies in multiple locations.

13.15 Retaining Control and Right to Intervene

- Retaining control and the right to intervene is an important aspect of IT service outsourcing to ensure that POLYCAB maintains oversight and can take necessary actions to protect its interests. These key aspects shall be considered for retaining control and the right to intervene in IT service outsourcing:
- Include specific contractual provisions that establish the organization's right to retain control and intervene in the outsourced activities. Clearly define the conditions under which intervention may be necessary, such as non-compliance with agreed-upon service levels, security breaches, or business continuity disruptions.
- Develop comprehensive SLAs that outline the performance standards, deliverables, and expectations for the service provider. Specify the metrics for measuring performance and the

consequences for non-compliance. Retain the ability to monitor and assess the service provider's performance against these SLAs and intervene if necessary.

- Establish a governance structure to oversee the outsourcing relationship. Assign dedicated personnel or a team responsible for monitoring the performance of the service provider. Define reporting mechanisms and regular review meetings to assess the service provider's adherence to contractual obligations and the organization's policies.
- Ensure that the organization retains the necessary access and control over its information, systems, and data. Define the requirements for data ownership, privacy, and security in the outsourcing agreement. Specify the organization's right to audit the service provider's processes, infrastructure, and security controls.
- Retain control over the change management processes associated with the outsourced activities. Define the approval mechanisms, change control procedures, and the organization's role in assessing and approving changes proposed by the service provider. Ensure that changes are aligned with the organization's strategic objectives and do not introduce unnecessary risks.
- Define escalation procedures and mechanisms for resolving disputes or conflicts that may arise during the outsourcing relationship. Establish clear channels of communication and define the hierarchy of escalation for different types of issues. Retain the ability to escalate matters to senior management or terminate the agreement if necessary.
- Protect the organization's intellectual property rights by clearly defining ownership and usage rights in the outsourcing agreement. Ensure that the service provider adheres to confidentiality obligations and safeguards the organization's proprietary information. Retain the ability to intervene if there are concerns regarding the protection of intellectual property.
- Conduct periodic assessments and audits to evaluate the service provider's compliance with contractual obligations, security standards, and industry best practices. Retain the right to perform independent audits or engage third-party auditors to assess the service provider's processes, controls, and performance.
- Include exit strategies and termination clauses in the outsourcing agreement to ensure a smooth transition in case of non-performance or termination of the agreement. Retain control over the transition process, including data migration, knowledge transfer, and the re-establishment of services in-house or with an alternative provider.

13.16 Communication and Escalation

Communication and escalation play a crucial role in IT service outsourcing to ensure effective collaboration, timely issue resolution, and the ability to intervene when necessary. The following are key considerations for communication and escalation to intervene in IT service outsourcing shall be followed:

- Define clear and accessible communication channels between the organization and the service provider. Establish primary and secondary points of contact for both parties. Ensure that contact information is up to date and readily available to all relevant stakeholders. Use multiple modes of communication, such as email, phone, and collaboration tools, to ensure effective communication.
- Establish reporting mechanisms that outline the frequency, format, and content of status updates, incident reports, and performance metrics. Define the reporting responsibilities of both the organization and the service provider. Specify the information that should be included in the reports, such as service level achievements, incidents, vulnerabilities, and upcoming changes.

- Schedule regular review meetings to discuss performance, service delivery, and ongoing projects. These meetings provide an opportunity to review the service provider's performance against agreed-upon SLAs, address any concerns or issues, and align on priorities. Review meetings also enable proactive discussions on improvements, innovations, and strategic alignment.
- Incident Management processes shall be established that allow for prompt reporting and resolution of issues. Define the procedures for reporting incidents, including the required information and the severity levels. Establish escalation paths based on the severity and impact of incidents. Ensure that the service provider promptly notifies the organization of any incidents and engages in a collaborative resolution process.
- Clear escalation procedures shall be defined to address issues that require higher-level intervention. Establish an escalation matrix that outlines the levels of escalation, responsible parties, and expected response times at each level. Clearly communicate the escalation procedures to both the organization and the service provider. Ensure that escalation paths are readily accessible and understood by all stakeholders.
- Identify the triggers that warrant escalation and intervention. These triggers may include significant service disruptions, repeated failures to meet SLAs, breaches in security or data protection, unresolved conflicts, or failure to address critical issues within defined timeframes. Clearly communicate these triggers to the service provider and establish protocols for escalating and addressing such situations.
- Ensure that the service provider acknowledges and responds to communication and escalations in a timely manner. Establish response timeframes and expectations for acknowledging and addressing issues. The organization should also commit to providing necessary information, approvals, or resources in a timely manner to facilitate the resolution process.
- Identify the key stakeholders within the organization who should be involved in communication and escalation processes. This may include senior management, IT leaders, project managers, and other relevant personnel. Clearly define their roles and responsibilities in the escalation and intervention process.

13.17 Data Backup and Recovery

Data backup and recovery are critical aspects in IT service outsourcing at POLYCAB for ensuring the protection and availability of POLYCAB data. The following considerations for data backup and recovery in IT service outsourcing: The following details shall be considered for data backup and recovery in IT service outsourcing.

- Specify the frequency of data backups in the outsourcing agreement. Determine how often backups should be performed based on the criticality of the data and the frequency of changes. Backup schedules can range from daily to hourly, depending on the organization's requirements and the service provider's capabilities.
- Define the backup strategy, which may include a combination of incremental and full backups. Incremental backups capture only the changes made since the last backup, reducing backup time and storage requirements. Full backups capture all data, ensuring a complete restore point. Determine the appropriate balance between incremental and full backups based on data volume, recovery objectives, and resource constraints.
- Specify the duration for which backups should be retained. Consider regulatory requirements, legal obligations, and business needs when defining the retention period. Ensure that the

service provider adheres to the defined retention period and has appropriate storage infrastructure to retain backups securely.

- Evaluate the need for off-site or cloud-based backup solutions to enhance data protection. Off-site backups provide an additional layer of resilience by storing copies of data at a geographically separate location. Cloud backup solutions offer scalability, accessibility, and automated backup processes. Determine the suitability of off-site or cloud backup options based on security, compliance, and business requirements.
- Ensure that the service provider validates the integrity and completeness of backups regularly. Regularly test the restoration process to confirm that backups can be successfully restored, and data integrity is maintained. Perform periodic checks and audits to verify the consistency and reliability of backups.
- Ensure that backups are encrypted to protect sensitive data during transit and storage. Specify the encryption standards and protocols that the service provider should adhere to. Encryption helps safeguard data from unauthorized access or breaches during the backup and recovery process.
- Mandate regular testing of the disaster recovery processes and procedures. Conduct simulated disaster recovery drills to validate the effectiveness and efficiency of the recovery mechanisms. Test different scenarios and recovery options to ensure readiness and identify any gaps or areas for improvement.
- Implement robust change management processes to ensure that changes to data systems and configurations do not affect the ability to recover data. Coordinate with the service provider to ensure that data backups are performed before significant changes are implemented. Maintain data consistency across backup sets to avoid data corruption or inconsistencies during the recovery process.
- Clearly outline the service provider's responsibilities regarding data backup and recovery in the outsourcing agreement. Specify their obligations to perform regular backups, store backups securely, validate backups, and adhere to agreed-upon RTO and RPO targets.
- Ensure that the service provider has appropriate disaster recovery capabilities and infrastructure.

13.18 Alternative Service Providers

Identifying and having alternative service providers is an important factor at POLYCAB for IT service outsourcing to mitigate risks and ensure continuity of operations.

The following considerations for having alternative service providers in IT service outsourcing:

- During the vendor evaluation and selection process, consider potential alternative service providers as part of your due diligence. Identify multiple vendors who have the capabilities and expertise to provide similar services. Evaluate their track record, reputation, financial stability, technical capabilities, and service offerings to assess their suitability as potential alternatives.
- Ensure that alternative service providers can seamlessly integrate into your existing IT infrastructure and systems. Assess their compatibility with your current technology stack, data formats, and interfaces. Evaluate their ability to handle the scale and complexity of your IT requirements. Define transition processes and expectations to ensure a smooth transfer of services in case of the need to switch providers.
- Include provisions in the outsourcing agreement that allow for the engagement of alternative service providers. Clearly define the conditions under which alternative providers can be

engaged, such as non-performance, breach of contract, or other predefined triggers. Address legal and compliance considerations, such as data protection, intellectual property rights, and confidentiality, to ensure a smooth transition.

- Conduct a comprehensive risk assessment of alternative service providers to ensure their reliability, resilience, and ability to meet your business needs. Perform due diligence to evaluate their financial stability, reputation, security practices, and compliance with regulatory requirements. Consider factors such as their geographical location, data centers, disaster recovery capabilities, and business continuity plans.
- Proactively build relationships with potential alternative service providers. Establish regular communication channels and foster a collaborative partnership with them. Conduct periodic meetings, site visits, and technical discussions to stay informed about their capabilities, service offerings, and any updates or changes that may impact their suitability as an alternative provider.
- Define exit strategies in the outsourcing agreement to facilitate the transition to alternative service providers, if needed. Include provisions for data migration, knowledge transfer, and the transfer of assets or infrastructure. Clearly outline the responsibilities of both parties during the transition period and ensure that the exit process does not disrupt ongoing operations.

14. DR Setup and Strategy

14.1 DR Setup

Currently the DR site host only business critical applications as identified through Business Impact Analysis data and is not a full replica of primary site. Both Primary and DR sites are accessible over MPLS/P2P/Internet/Site-to-Site VPN from all locations of POLYCAB. The primary and DR sites are connected by dual point to point links.

POLYCAB has deployed VPN solution for enabling users to connect over internet to access the applications and network drives hosted in the Data center. Currently, this has been made available to the critical users from Corporate office.

14.2 DR Strategy

POLYCAB uses native database replication techniques for data replication between the primary.

and DR sites. Changes to application are deployed by the Application team to DR within two days from deployment in production site.

14.3 Backup Procedure

Adequate controls for data backup are defined in the Backup Policy and the backup and recovery procedures maintained by the IT Team Backups are taken on regular basis to ensure data is available in the event of disaster or for recovering old transactions.

The components backed up but not limited for respective applications are as follows:

- Application files
- Critical file server data
- Data files
- Emails

- Configuration files (Network devices, firewall rule base, etc.)
- Databases
- Log files including operating system logs, application logs and security logs.
- Production application & database server's backups are done on daily basis on disk.

Post which application server's backup are written on disk (D To D) using storage solution on daily, weekly & monthly basis.

14.4 Planning BCP-DR Drill

The DRBCP Team shall plan and organize periodical DR drills, to ensure that the plan works on the ground as intended and is consistent with the scope and objectives of DRBCP at the POLYCAB.

At the minimum, the DR-BCP drill is conducted every quarter.

The BCP Coordinator shall plan and arrange for the required number of drills at the stated periodicity or as and when asked for with assistance from other BCP coordinators, if any.

The Drill report and results shall be reported to the Management Team. Learnings from the same shall be utilized to revise the DRBCP, if required.

14.5 Testing Strategy

POLYCAB shall conduct DR Drills/live training from DR site shall include running all operations from DRS.

15. Awareness & Training

The success of the DRBCP depends on employees' awareness of the processes and services in addition to the activities to be carried out to guarantee their continuity at the time of disaster.

POLYCAB may set up an ongoing training and information process (Awareness) aimed at promoting awareness regarding the importance of the Business Continuity among the staff which may also include both the management staff in charge of updating the plans and the operative staff who must perform the various activities indicated by the plans themselves.

Creating awareness of the BCP shall also be done by:

- Sending awareness emails to all POLYCAB employees
- Holding brief meetings of the emergency team members to reiterate the responsibilities.
- Performing simulation exercise so that employees receive practical experience via testing of BCP.

- The below staff earmarked as ER staff and BC Coordinators shall undergo formal BCP Training along with BC Manager

S. No.	Department	ER Staff / BC Coordinator
1	IT	
2	Cyber Security	
3	HR	
4	Admin	

5	Finance	
6	Digital	

16. BCP / DR Testing

- BCP/ DR plan is reviewed on a yearly basis or in case of a major change in business or infrastructure.

17. Enforcement

- Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.
- Polycab will take appropriate legal action against any individual or organization that causes harm to Polycab.

18. Training and Awareness

- The Cyber Security team shall conduct necessary awareness campaigns to sensitize the employees, contractors, vendors, and third-party partners about Polycab data security policies.

19. Review and Update

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

20. Annexure

- DR Procedure

025 - Disaster Recovery Procedure

- DR Plan

DR Plan Temaplte

21. Reference

ISO 27001 Reference

- 5.30 ICT readiness for business continuity