

Business Continuity Plan (BCP)

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Version: 1.4

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Document Revision History:

VERSION NO.	REVISION DATE	AUTHOR	REVIEWED BY	APPROVED BY	DESCRIPTION
1	26/6/2020	P.Sahoo	Ranjeet Singh	Amit Sobti	Reviewed
1.1	28/6/2021	P.Sahoo	Ranjeet Singh	Amit Sobti	Reviewed
1.2	28/6/2022	P.Sahoo	Rajat Ghosh	Amit Sobti	Reviewed
1.3	28/6/2023	P.Sahoo	Rajat Ghosh	Amit Sobti	Reviewed
1.4	28/7/2024	P.Sahoo	Shankar VRG	Amit Sobti	Reviewed

1. Executive Summary

The Business Continuity Plan (BCP) aims to prepare BPO Convergence Pvt.Ltd to maintain essential business operations during unforeseen disruptions, whether due to natural disasters, cyberattacks, equipment failure, or other unforeseen events. This plan ensures that critical business functions, employees, customers, and suppliers are supported during an emergency, while recovery efforts are streamlined to restore normal operations as quickly as possible.

2. Objectives

- Ensure the continuation of critical business functions during and after any disruption.
- Minimize financial losses and operational downtime during unforeseen events.
- Preserve the organization's reputation and ensure service levels are met during crises.
- Ensure quick recovery of IT systems, infrastructure, and data, to ensure business processes continue with minimal interruptions.

3. Scope

The scope of this plan covers:

- **Critical Business Functions:** Operations that directly affect the organization's ability to serve its clients and meet contractual obligations.
- **Personnel and Resources:** Identifying key personnel, resources, and recovery facilities.
- **Technology Infrastructure:** Ensuring IT systems, data centers, communication systems, and software are secure and operational during and after a crisis.
- **Communication Protocols:** Defining how communication will occur internally and externally during emergencies.

4. Risk Assessment

An initial risk assessment will identify the most likely threats to the business, including:

- **Natural Disasters:** Earthquakes, floods, hurricanes, etc.
- **Cybersecurity Threats:** Ransomware, data breaches, DDoS attacks.
- **Hardware Failures:** Server, network, or storage failures.
- **Human Error:** Accidental data deletion, misconfigurations, etc.
- **Pandemics:** Impact of widespread illness on workforce availability.
- **Power Failures:** Unforeseen power outages or loss of electricity supply.

5. Critical Business Functions

The following business functions are vital for the organization's survival and must be maintained or rapidly restored in the event of a disruption:

- **Customer Service:** Handling customer queries and complaints through phone, email, and chat support.
- **Sales and Order Processing:** Ensuring customer orders are fulfilled and payments are processed.
- **Finance and Payroll:** Managing payroll, financial transactions, and invoicing.

- **IT and Data Recovery:** Ensuring the security and availability of data, applications, and IT systems.
- **Human Resources:** Managing staffing levels, roles, and responsibilities during a crisis.

6. Recovery Strategy

The recovery strategy ensures that key operations and IT systems can resume as quickly as possible after a disruption:

- **Business Function Continuity:**
 - **Alternate Work Locations:** In case of office closure, employees will work remotely or from an alternative office location.
 - **Remote Access Systems:** Secure Virtual Private Network (VPN) access will be provided for all critical employees.
 - **Outsourcing of Non-Critical Operations:** Non-essential operations may be temporarily outsourced or paused to focus on critical services.
- **Data Backup and Recovery:**
 - **Backup Frequency:** Full backups are taken weekly, and incremental backups are taken daily.
 - **Data Storage:** Backups are stored in a combination of on-site servers and cloud storage (AWS, Azure).
 - **Data Recovery:** In case of data loss or corruption, recovery procedures are in place to restore from the most recent backup.
- **IT System Failover:**
 - **Hot Sites:** A fully operational secondary data center (hot site) is maintained for failover in case of data center failure.
 - **Cloud-Based Solutions:** The organization relies on cloud-based solutions for critical systems to ensure accessibility during disruptions.
- **Communication:**
 - **Internal Communication:** Use of email, phone, and messaging apps to keep all employees informed about the situation.

- Customer Communication: A designated communication team will notify customers via email, social media, and the website.
- Supplier and Vendor Communication: Communication protocols with suppliers to ensure continued supply chain operations or contingency plans if suppliers are affected.

7. Business Continuity Procedures

The following steps outline how operations will continue during a disaster:

1. Incident Detection:

- Monitor for potential disruptions (system failure, natural disaster, etc.).
- Immediate notification of the Business Continuity Team.

2. Activation of the BCP:

- The Business Continuity Manager will activate the BCP and notify the team.
- Notify all stakeholders, including employees, customers, suppliers, and partners.

3. Disaster Recovery Execution:

- **Operational Recovery:** Shift to alternate work locations or work-from-home setups. Ensure critical business operations resume within 1-2 hours.
- **IT Recovery:** Activate cloud backup and restore data from recent backups. Deploy failover systems (hot site or cloud infrastructure) to restore operations.
- **Communication:** Update employees regularly through internal communication channels. Notify customers and vendors about the incident and recovery progress.

4. Post-Recovery Analysis:

- Conduct a thorough assessment of the disaster event and response process.
- Identify areas for improvement and update the plan as necessary.

8. Testing and Drills

The Business Continuity Plan will be tested annually to ensure readiness. Testing includes:

- **Tabletop Exercises:** Scenario-based drills where team members discuss their actions during a disaster.
- **Simulation Tests:** Full-scale tests involving the actual execution of the recovery plan to ensure systems and personnel are prepared.
- **Plan Review and Updates:** After each test or actual event, the plan will be reviewed and updated as needed.

9. Plan Maintenance

The Business Continuity Plan will be reviewed and updated regularly to reflect any organizational changes, technological advancements, or new business risks. The plan will be:

- **Reviewed annually** by the Business Continuity Team.
- **Updated** whenever major changes occur in technology, business structure, or operations.
- **Version-controlled** to keep track of all modifications.

Conclusion

The **Business Continuity Plan (BCP)** ensures that BPO Convergence Pvt.Ltd is prepared to handle disruptions effectively, maintaining key operations and ensuring rapid recovery. The plan defines roles, responsibilities, and processes necessary for business survival in the event of any crisis, ensuring that we can minimize downtime and maintain customer trust.