

Disaster Recovery Plan (DRP)

(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 purpose of this Disaster Recovery Plan (DRP) is to establish a framework for the recovery and continuity of critical business operations and IT infrastructure in the event of a disaster. This plan provides step-by-step procedures for identifying, responding to, and recovering from various disaster scenarios to ensure minimal downtime and business impact.

2. Objectives

- To restore IT operations and business processes as quickly as possible after a disaster.
- To minimize data loss by maintaining appropriate backup systems and strategies.
- To ensure that critical business functions can continue with minimal disruption.
- To document roles and responsibilities during a disaster recovery effort.

3. Scope

This plan covers the following:

- IT systems, applications, and data critical to business operations.
- Communication systems (email, phone, messaging).
- Backup systems and recovery strategies.
- Physical infrastructure such as data centers and office facilities.
- Vendor and third-party service recovery processes.

4. Risk Assessment

The organization faces several risks that could lead to operational disruptions:

- Natural Disasters: Earthquakes, floods, hurricanes, etc.
- Cyber Threats: Malware, ransomware, DDoS attacks, data breaches.
- Hardware Failures: Server crashes, storage failures, network issues.
- Human Error: Accidental deletion of critical data, misconfigurations.
- Power Failures: Loss of electricity, backup generator failure.

5. Critical Business Functions

The following business functions are critical and must be restored immediately after a disaster:

- Customer Support: Handling customer inquiries and complaints.
- Order Management System: Processing and fulfilling customer orders.
- Financial Systems: Managing payroll, invoicing, and financial transactions.
- Email and Communication: Internal communication for business continuity.
- Data Access and File Storage: Access to critical business files and databases.

7. Recovery Strategy

The recovery strategy defines how to restore critical systems, applications, and data in the event of a disaster:

- **Data Backup:**
 - Full backups of critical data are taken weekly.
 - Incremental backups are taken daily.
 - Backups are stored both on-site and off-site (cloud storage).
 - Backups are encrypted using AES-256 encryption to ensure data security.
- **System Recovery:**
 - Primary Data Center: Use of primary on-site systems for recovery.
 - Secondary Data Center (Hot Site): In case of a total loss, systems will failover to a secondary data center, where data is replicated in real-time.
 - Cloud Services: Leveraging cloud infrastructure (AWS, Azure) for scalable recovery options.
- **Communication Plan:**
 - Internal Communication: Employees will be informed via email, SMS, and phone.
 - External Communication: Customer-facing communication will be done through the website, social media, and email newsletters.
- **Vendor Recovery:**
 - Pre-arranged agreements with third-party vendors for quick restoration of internet, power, telephony, and SaaS solutions.

8. Recovery Procedures

The following procedures will be followed in the event of a disaster:

1. Incident Identification:

- The IT team will immediately assess the situation (e.g., power failure, internet outage, cyberattack, etc.).
- The Disaster Recovery Manager will be notified to activate the plan.

2. Activate DRP:

- The Disaster Recovery Manager will declare a disaster and initiate the recovery plan.
- Notify the disaster recovery team and stakeholders.

3. Recovery Execution:

- **Restore Data:** Start data restoration from the most recent backup.
- **System Recovery:** Boot up servers, applications, and services in the failover systems (e.g., secondary data center or cloud).
- **Communication:** Internal updates will be provided to employees. Customer communication will be made available on the website or via email.
-

4. Post-Recovery Evaluation:

- Assess the situation and document lessons learned.
- Conduct a debriefing session with the recovery team to identify areas for improvement.

9. Backup and Storage

The backup systems in place are designed to ensure data availability and security:

- **Backup Frequency:**
 - Full backups every Sunday at midnight.
 - Incremental backups every night.
- **Off-site Storage:**

Backups are stored in the cloud (e.g., AWS S3, Azure Blob Storage) with AES-256 encryption for security.
-
- **Retention Period:**

- Backups are retained for 30 days. Older backups are archived for long-term storage.

10. Testing and Validation

The Disaster Recovery Plan will be tested semi-annually using the following methods:

- **Tabletop Exercise:** A scenario-based discussion involving key personnel to walk through the DRP.
- **Full-Scale Test:** A simulation where all systems are tested under real disaster conditions, including data recovery and system failover.
- **Post-Test Evaluation:** Results of the test will be reviewed, and the plan will be updated accordingly based on lessons learned.

11. Plan Maintenance

The DRP will be reviewed and updated annually or when significant changes occur to infrastructure, personnel, or business operations. The following steps are involved:

- **Annual Review:** Review the DRP document to ensure its relevance.
- **Update Procedures:** Any significant changes (e.g., new systems, software, personnel) will trigger an update to the plan.
- **Version Control:** Track updates and revisions to the DRP to ensure documentation is up to date.

Conclusion

The Disaster Recovery Plan (DRP) ensures that BPO Convergence Pvt.Ltd is prepared for a wide range of disaster scenarios. This plan includes well-documented recovery procedures, clear roles and responsibilities, and effective backup strategies to guarantee business continuity.