BWEvents LLC
Disaster Recovery Plan

Revision History

Version	Date	Author	Description of changes
1.0	02/01/2022	Satish Baniya	Initial Release
1.1	05/01/2023	Satish Baniya	Review and updates

1. Executive Summary:

The Disaster Recovery Plan (DRP) of BWEvents Tech outlines the strategies, procedures, and responsibilities required to recover critical IT systems and data in the event of a disaster or significant technology-related incident. This plan aims to minimize downtime, restore services promptly, and protect business continuity.

2. Scope and Objectives:

The scope of this plan includes all IT systems, applications, and data critical to BWEvents Tech's operations. The primary objectives are to:

- Ensure the rapid recovery of IT systems and data to minimize business disruptions.
- Establish clear roles and responsibilities for the IT disaster recovery process.
- Ensure data integrity, confidentiality, and availability during the recovery process.
- Test and maintain the effectiveness of the disaster recovery procedures regularly.

3. Risk Assessment and Impact Analysis:

A comprehensive risk assessment and impact analysis have been conducted to identify potential threats to IT systems and data. The analysis has helped determine the prioritization of recovery efforts based on the criticality of systems and data.

4. Disaster Recovery Team:

The Disaster Recovery Team (DRT) is responsible for developing, implementing, and maintaining this DRP. The team includes representatives from IT, security, operations, and management.

5. Disaster Recovery Strategies:

5.1. Data Backup and Recovery:

Critical data will be regularly backed up and stored securely in an off-site location. Backup schedules will align with the Recovery Point Objectives (RPOs) identified in the risk assessment.

5.2. Redundancy and Failover:

Where applicable, redundant systems will be implemented to ensure high availability. Failover mechanisms will be activated in case of primary system failures.

5.3. Cloud Services:
Cloud-based solutions will be utilized to store critical data and services, ensuring accessibility and scalability during a disaster.

6. Incident Response and Escalation:
An incident response process will be followed to address disasters promptly. The IT team will escalate incidents to the Disaster Recovery Team, who will coordinate the recovery efforts.

7. Disaster Recovery Procedures:
The DRP includes detailed step-by-step procedures for recovering IT systems and data. These procedures cover hardware replacement, data restoration, system configuration, and testing.

8. Communication Plan:
A Communication Plan will ensure that stakeholders, including employees, customers, and partners, are informed promptly during the disaster recovery process.

9. Training and Awareness Program:
Regular training sessions will be conducted for IT staff to ensure they are familiar with their roles and responsibilities during disaster recovery efforts.

10. Testing and Maintenance:
The Disaster Recovery Plan will be tested through regular exercises and simulations. Testing will be done in a controlled environment to identify potential weaknesses and improve recovery capabilities.

11. Documentation and Records Management:
All Disaster Recovery documents, including this plan and related procedures, will be properly documented, maintained, and accessible to authorized personnel through secure storage.

12. Governance and Review:
The Disaster Recovery Team will conduct periodic reviews and updates of the plan to ensure its relevance and effectiveness. Changes to the plan will be approved by management.

13. Plan Activation and Deactivation:
The DRP will be activated when a disaster or significant IT incident occurs. Upon successful recovery and restoration of IT systems, the DRP will be deactivated, and normal operations will resume.

14. Compliance:
All IT staff are required to comply with the provisions of this Disaster Recovery Plan. Non-compliance may result in disciplinary actions.