Information Technology Disaster Recovery Plan (DRP)

Table of Contents

1. Purpose and Scope

The purpose of this Disaster Recovery Plan (DRP) is to establish procedures to recover the company's critical information technology systems in the event of a disaster or significant disruption. The plan ensures the continuity of business operations by restoring IT services in a timely and organized manner.

This DRP applies to all critical IT systems, including servers, networks, applications, databases, and data storage systems. It covers both natural and man-made disasters, such as data breaches, hardware failures, power outages, and environmental hazards.

2. Objectives

1. Minimize downtime: Ensure rapid recovery of critical systems to reduce business disruption.
2. Protect data integrity: Safeguard and recover company data with minimal loss or corruption.
3. Define roles and responsibilities: Ensure clear accountability and coordination during recovery efforts.
4. Ensure business continuity: Enable ongoing operations with a focus on restoring essential services first.
5. Comply with regulations: Meet legal, regulatory, and contractual obligations related to disaster recovery and data protection.

3. Roles and Responsibilities

3.1 Disaster Recovery Team (DRT)

The Disaster Recovery Team (DRT) is responsible for executing the disaster recovery plan. The team includes personnel from IT, management, communications, and any other relevant departments.

1. Disaster Recovery Coordinator: Oversees the execution of the DRP and coordinates all recovery activities.
2. IT Infrastructure Lead: Responsible for technical recovery of servers, networks, and critical hardware.
3. Application Recovery Lead: Manages recovery and testing of applications and databases.
4. Backup and Data Recovery Lead: Oversees backup integrity and data restoration.
5. Communication Officer: Handles internal and external communication during the disaster recovery process.

3.2 Senior Management

Senior management ensures that sufficient resources and support are available for disaster recovery efforts. They make decisions about business continuity, disaster declaration, and communication with external parties.

4. Disaster Recovery Procedures

4.1 Risk Assessment

A risk assessment must be conducted annually to identify potential disaster scenarios that could disrupt IT services. The assessment includes:

1. Identification of critical systems, applications, and data.
2. Analysis of potential risks (natural disasters, cyberattacks, power failures, etc.).
3. Evaluation of the impact of downtime on business operations.

4.2 Disaster Types and Recovery Strategy

Different types of disasters require tailored recovery strategies, including:

1. Natural Disasters: Such as earthquakes, floods, or fires. Physical facilities and backup data centers may be affected.
2. Cybersecurity Incidents: These include data breaches or ransomware. Immediate isolation of affected systems and data restoration will be necessary.
3. Hardware/Software Failures: Such as server crashes or software corruption. Data restoration and system reboot will be required.
4. Human Error: Accidental deletion of data or misconfiguration of systems will involve a review of logs and recovery of backup data.

4.3 Disaster Declaration

A disaster must be declared when a critical system failure or event severely disrupts business operations or when the potential for prolonged downtime is identified. The decision to declare a disaster is made by the Disaster Recovery Coordinator in consultation with senior management.

4.4 Recovery Team Activation

1. Upon declaring a disaster, the Disaster Recovery Coordinator will activate the Disaster Recovery Team (DRT). Each team member must:
2. Assess the extent of the damage or disruption.
3. Report on the status of critical systems and infrastructure.
4. Implement recovery procedures in accordance with the DRP.

4.5 Communication Plan

1. Effective communication is crucial during the disaster recovery process. The Communication Officer will:
2. Notify all employees and stakeholders of the disaster and provide regular updates on the recovery process.

3. Communicate with vendors and service providers as necessary.
4. Handle media inquiries and public statements, if applicable.

5. Backup and Restoration Procedures

5.1 Backup Process

1. Daily Backups: All critical data must be backed up daily. Backups should include full copies of databases, file systems, and application data.
2. Backup Locations: Backups must be stored in both on-site and off-site locations, with a preference for cloud storage for geographic redundancy.
3. Backup Integrity: Regular integrity checks must be conducted to ensure the backup data is not corrupt or incomplete.

5.2 Data Restoration

Step 1: Verify the cause of the disaster and assess data loss.
Step 2: Identify the most recent, uncompromised backup and initiate data restoration.
Step 3: Recover databases, applications, and configurations in priority order, based on the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) defined for each system.
Step 4: Validate the integrity and functionality of restored systems before allowing business operations to resume.

6. Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

6.1 Recovery Time Objective (RTO)

The RTO defines the maximum acceptable amount of time that critical systems can be offline before business operations are significantly impacted. The RTO for each critical system is determined based on the business impact analysis.

SYSTEM	**RTO**
Financial systems	4 hours
Member-facing websites	2 hours
Internal communication systems	6 hours
Non-critical systems	48 hours

6.2 Recovery Point Objective (RPO)

The RPO defines the maximum acceptable amount of data loss measured in time. It is the age of files or transactions that must be recovered from backup storage.

SYSTEM	RTO
Financial systems	30 minutes
Member-facing websites	15 minutes
Internal communication systems	1 hour
Non-critical systems	24 hours

7. Testing and Maintenance

7.1 Disaster Recovery Testing

1. Annual Testing: The Disaster Recovery Plan must be tested at least once per year to ensure that recovery procedures can be executed efficiently.
2. Scenario Testing: The testing should simulate various disaster scenarios, including hardware failures, cyberattacks, and data loss events.
3. Documentation: Results of each test must be documented, including any issues encountered and lessons learned for plan improvements.

7.2 Plan Maintenance

Annual Review: The DRP must be reviewed annually and updated to reflect changes in IT infrastructure, business operations, or regulatory requirements.

Team Updates: Contact information for the Disaster Recovery Team must be kept up to date, and any personnel changes must be communicated immediately.

8. Plan Review and Revision

This Disaster Recovery Plan must be reviewed and revised regularly to ensure its effectiveness and relevance. The IT department, in coordination with senior management, is responsible for ensuring that the plan reflects the current state of the company's IT infrastructure and business priorities. Any changes in business processes, IT systems, or regulatory requirements should trigger a review and update of the DRP.

Last Review Date: [Insert Date]
Next Scheduled Review: [Insert Date]

This IT Disaster Recovery Plan is essential for ensuring the resiliency and continuity of business operations. It is the responsibility of all relevant personnel to understand their roles and execute this plan in the event of a disaster.