<Logo>

<Organization Name>

**Disaster Recovery Plan**

|  |  |
| --- | --- |
| **Standard** | ISO/IEC 27001:2022 |
| **Version** | <Version> |
| **Prepared By** | <Name> |
| **Approved by** | <Name of Approval Authority/Board> |
| **Date Approved** | <Approval Date> |
| **Next Review Date** | <Review Date (typically a year from the approval date)> |
| **Document Classification** | Confidential/Public/Internal Use Only |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision History** | | | | |
| **Version** | **Date** | **Prepared By** | **Approved By** | **Changes/Notes** |
| <version No> | <DD/MM/YYYY> | <Name> | <Name> | *Initial Version* |

|  |  |  |
| --- | --- | --- |
| **Distribution List** | | |
| **Recipient Name** | **Department** | **Distribution Date** |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision History** | | | | |
| **Version** | **Date** | **Prepared By** | **Approved By** | **Changes/Notes** |
| <version No> | <DD/MM/YYYY> | <Name> | <Name> | *Initial Version* |

|  |  |  |
| --- | --- | --- |
| **Distribution List** | | |
| **Recipient Name** | **Department** | **Distribution Date** |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |

**Table of Contents**

[Purpose 7](#_Toc179812797)

[Scope 7](#_Toc179812798)

[Objectives 7](#_Toc179812799)

[Roles and Responsibilities 8](#_Toc179812800)

[Disaster Scenarios and Response 8](#_Toc179812801)

[Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) 9](#_Toc179812802)

[Data Backup and Restoration Procedures Table 9](#_Toc179812803)

[Testing and Continuous Improvement 10](#_Toc179812804)

[Communication Plan 10](#_Toc179812805)

[Plan Review and Maintenance 11](#_Toc179812806)

[Plan Maintenance Procedures 11](#_Toc179812807)

# Purpose

The purpose of this Disaster Recovery Plan is to outline the processes for recovering the IT infrastructure and services of <Organization Name> in the event of a disaster or significant disruptive incident. This plan ensures business continuity and aligns with the ISO 27001:2022 requirements.

# Scope

This plan applies to all critical IT services and systems within <Organization Name>, including data centers, cloud services, and essential IT infrastructure. It covers natural disasters, cyberattacks, system failures, and human errors.

# Objectives

* Ensure the rapid recovery of critical business operations.
* Minimize the downtime and impact on business operations.
* Safeguard critical data and maintain confidentiality, integrity, and availability.
* Ensure compliance with ISO 27001:2022 for disaster recovery and business continuity.

# Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| Disaster Recovery Team (DRT) | Leads recovery efforts and coordinates the implementation of the recovery plan. |
| IT Department | Manages backup systems, ensures data recovery, and infrastructure restoration. |
| CISO/IT Security Lead | Ensures security controls are maintained during recovery. |
| HR and Communications | Manages internal and external communication during the recovery process. |
| <Role> | <Responsibility> |
| <Role> | <Responsibility> |

# Disaster Scenarios and Response

|  |  |
| --- | --- |
| **Disaster Scenario** | **Response** |
| Cyberattack (Ransomware) | Isolate affected systems, restore data from backup, notify regulatory bodies. |
| Natural Disaster (Flood/Fire) | Move operations to an alternate site, restore critical systems, and ensure staff safety. |
| Data Loss or Corruption | Retrieve latest backups, restore systems, and ensure data integrity checks. |
| <Scenario> | <Response> |
| <Scenario> | <Response> |

# Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)

|  |  |  |
| --- | --- | --- |
| **System** | **RTO** | **RPO** |
| Core ERP System | *4 hours* | *1 hour* |
| Email and Communication | <Time in hours> | <Time in hours> |
| Client Database | <Time in hours> | <Time in hours> |
| <System> | <Time in hours> | <Time in hours> |
| <System> | <Time in hours> | <Time in hours> |

# Data Backup and Restoration Procedures Table

|  |  |
| --- | --- |
| **Procedure** | **Details** |
| Backup Frequency | Daily backups of all critical data are stored offsite and in the cloud. |
| Backup Storage Locations | Offsite facility and cloud storage to ensure data redundancy and security. |
| Backup Retention Period | Backup data is retained for a period of 90 days, after which it is archived. |
| Backup Testing Frequency | Backup systems are tested quarterly to verify data integrity and restore functionality. |
| Restoration Process | In the event of data loss, recovery will be initiated from the latest verified backup. |
| Recovery Point Objective (RPO) | The maximum acceptable amount of data loss measured in time (e.g., 1 hour). |
| Restoration Timeframe | Restoration must be completed within the designated RPO timeframe (e.g., 4 hours). |
| Verification of Restoration | After restoration, systems are verified for data accuracy and completeness. |

**Backup Frequency** - Daily backups ensure minimal data loss in case of incidents.

**Testing** - Quarterly tests ensure that backups are functional and can be restored successfully.

**Restoration Process** - Ensures quick recovery and continuity after data loss, based on the most recent verified backups.

# Testing and Continuous Improvement

**Regular Testing**

Disaster recovery tests are conducted annually to evaluate the plan’s effectiveness and update it as necessary.

**Post-Disaster Review**

After each recovery incident, the plan will be reviewed, and lessons learned will be integrated into future iterations.

# Communication Plan

|  |  |  |
| --- | --- | --- |
| **Internal Communication** | **Responsible** | **Method** |
| Incident Response Updates | DRT Lead | *Email, Internal Portal* |
| Employee Notifications | HR Department | *Phone, SMS, Microsoft Teams* |
| <Internal Communication> | <Department> | <Communication Method> |
| <Internal Communication> | <Department> | <Communication Method> |

|  |  |  |
| --- | --- | --- |
| **External Communication** | **Responsible** | **Method** |
| Regulatory Notifications | Legal Team | *Official Letter, Email* |
| Client Updates | Client Relations | *Email, Phone* |
| <External Communication> | <Department> | <Communication Method> |
| <External Communication> | <Department> | <Communication Method> |

# Plan Review and Maintenance

The **Disaster Recovery Plan** must be regularly reviewed and updated to ensure its effectiveness and relevance to the organization’s operations. This section outlines the procedures and conditions under which the plan must be maintained.

|  |  |
| --- | --- |
| **Review Frequency** | **Details** |
| Annual Review | The plan should be reviewed at least once every year to assess any changes in technology, risks, or operations. |
| Post-Incident Review | The plan should be reviewed and updated after any disaster recovery event or security incident, incorporating lessons learned. |
| Changes in IT Infrastructure | If there are significant changes in IT infrastructure, such as new systems, services, or cloud integrations, the plan must be updated accordingly. |
| Changes in Organization Structure | Any changes in organizational structure, personnel, or key responsibilities must trigger a review of the plan. |
| New Regulatory Requirements | Updates should be made to reflect any new legal or regulatory compliance requirements (e.g., data protection laws, industry standards). |
| Testing Results | The results of regular disaster recovery drills or testing should be analyzed, and the plan should be adjusted based on any gaps or improvements identified. |

## Plan Maintenance Procedures

* Any changes to the Disaster Recovery Plan must be documented, with a version history maintained to track revisions and updates.
* All relevant stakeholders must be notified of significant changes to the plan.
* If the plan undergoes substantial changes, staff involved in the Disaster Recovery process must be retrained.
* Maintain a version control log, ensuring that each update is recorded with following details.
  + Version number
  + Date of revision
  + Description of changes
  + Approval from responsible parties
* Regular internal audits should be conducted

**Appendix 2: Contact Information for Disaster Recovery Team**

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Contact Info** |
| <Name> | IT Lead | <Phone/Email> |
| <Name> | Security Lead | <Phone/Email> |
| <Name> | <Role> | <Phone/Email> |
| <Name> | <Role> | <Phone/Email> |