**Disclaimer:**

This IT Disaster Recovery Plan template is provided for general informational purposes only. It is not a substitute for professional advice, and users should adapt it to their specific needs and circumstances. While this template is based on best practices, L2 Cyber Security Solutions make no warranties or guarantees regarding its effectiveness or suitability for any particular situation. Users are responsible for ensuring the accuracy and completeness of the plan for their organisation. This template does not constitute legal advice, and users should consult with legal counsel for their specific legal needs. IT Disaster Recovery best practices evolve, and users are encouraged to stay updated on industry standards. It is crucial to regularly test and revise this plan to ensure its effectiveness.

**[Your Organisation Logo]**

**[Organisation Name]**

IT Disaster Recovery Plan (ITDRP)

Version: 1.0

Date: **[Date]**

Contents

[1. Executive Summary 4](#_Toc160441887)

[1.1 Purpose 4](#_Toc160441888)

[1.2 Scope 4](#_Toc160441889)

[1.3 Key Contacts 4](#_Toc160441890)

[1.4 Plan Objectives 4](#_Toc160441891)

[2. Introduction 4](#_Toc160441892)

[2.1 Background 4](#_Toc160441893)

[2.2 Document Overview 4](#_Toc160441894)

[3. Scope of this plan 4](#_Toc160441895)

[3.1 Systems/Technology included in the scope 4](#_Toc160441896)

[3.2 Systems/Technology that are out of scope 5](#_Toc160441897)

[4. Recovery Procedures 5](#_Toc160441898)

[4.1 Incident Response and Escalation 5](#_Toc160441899)

[4.2 Data Backup and Recovery 5](#_Toc160441900)

[4.3 System Restoration 5](#_Toc160441901)

[4.4 Communication and Notification 5](#_Toc160441902)

[5. Resource Allocation 5](#_Toc160441903)

[5.1 Allocation of Personnel 5](#_Toc160441904)

[5.2 Allocation of Equipment and Facilities 5](#_Toc160441905)

[5.3 Allocation of Financial Resources 6](#_Toc160441906)

[6. Testing and Maintenance 6](#_Toc160441907)

[6.1 Testing Schedule 6](#_Toc160441908)

[6.2 Test Scenarios 6](#_Toc160441909)

[6.3 Test Results and Improvements 6](#_Toc160441910)

[6.4 Plan Maintenance 6](#_Toc160441911)

[7. Training and Awareness 6](#_Toc160441912)

[7.1 Employee Training 6](#_Toc160441913)

[7.2 Awareness Programs 6](#_Toc160441914)

[8. Plan Review and Update 6](#_Toc160441915)

[8.1 Regular Review Schedule 6](#_Toc160441916)

[8.2 Post-Incident Review 6](#_Toc160441917)

[9. Appendices 6](#_Toc160441918)

[9.1 IT Staff Contact Information 6](#_Toc160441919)

[9.2 Vendor Contact Information 7](#_Toc160441920)

[9.3 IT Hardware listing 7](#_Toc160441921)

[9.4 Network Diagram 7](#_Toc160441922)

[9.5 Document Revision History 7](#_Toc160441923)

[9.6 Glossary of Terms 7](#_Toc160441924)

# 1. Executive Summary

## 1.1 Purpose

The IT Disaster Recovery Plan (DRP) is designed to ensure the resilience of IT systems and data in the face of disasters and disruptions by defining strategies, procedures, and responsibilities for effective response and recovery.

## 1.2 Scope

This plan covers all IT systems, data, and services critical to the organisation's operations.

## 1.3 Key Contacts

List key personnel and their contact information.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Mobile Number** | **Alternative contact** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 1.4 Plan Objectives

Outline the objectives of the IT DRP, including:

Minimising data loss and downtime.

Restoring IT systems and services.

Ensuring organisation continuity.

# 2. Introduction

## 2.1 Background

Provide a brief background explaining the need for an IT DRP, including recent incidents or events that highlight its importance.

## 2.2 Document Overview

Explain the structure and purpose of this document, guiding readers through its sections.

# 3. Scope of this plan

## 3.1 Systems/Technology included in the scope

List the most important hardware, cloud or connectivity that are covered under this plan. A list of desktops/laptops/printers will be provided in one of the appendices.

|  |  |  |
| --- | --- | --- |
| **Name** | **Make/Model/Version** | **Function** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 3.2 Systems/Technology that are out of scope

|  |  |
| --- | --- |
| **Name** | **Reason for exclusion** |
|  |  |
|  |  |
|  |  |
|  |  |

# 4. Recovery Procedures

## 4.1 Incident Response and Escalation

Outline the steps to be taken during the incident response phase, including escalation procedures.

## 4.2 Data Backup and Recovery

Explain the data backup and recovery procedures, including data storage locations and restoration processes.

|  |  |  |  |
| --- | --- | --- | --- |
| **Location of Backup** | **Responsibility** | **Backup Generation**(daily, weekly or monthly + Number of sets for each) | **Type of Backup**Full or Incremental |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 4.3 System Restoration

Detail the procedures for restoring IT systems and services to full functionality.

|  |  |  |
| --- | --- | --- |
| **Priority** | **Application/System Name** | **Recovery steps /****Link to Recovery Document** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 4.4 Communication and Notification

Explain the communication plan for informing stakeholders and employees during IT disasters.

# 5. Resource Allocation

## 5.1 Allocation of Personnel

Define the roles and responsibilities of IT staff during recovery efforts.

## 5.2 Allocation of Equipment and Facilities

Explain how equipment and facilities will be allocated and utilised during recovery.

## 5.3 Allocation of Financial Resources

Detail the allocation of financial resources for IT disaster recovery efforts.

# 6. Testing and Maintenance

## 6.1 Testing Schedule

Outline the schedule for regular IT DRP testing and exercises.

## 6.2 Test Scenarios

Describe various test scenarios that will be used to evaluate the effectiveness of the plan.

## 6.3 Test Results and Improvements

Explain how test results will be documented and used to improve the IT DRP.

## 6.4 Plan Maintenance

Specify the process for updating and maintaining the IT DRP to reflect changes in the IT environment.

# 7. Training and Awareness

## 7.1 Employee Training

Explain the training programs in place to ensure that IT staff understand their roles in the IT DRP.

## 7.2 Awareness Programs

Detail awareness initiatives aimed at promoting a culture of IT disaster preparedness.

# 8. Plan Review and Update

## 8.1 Regular Review Schedule

Outline the schedule for reviewing and updating the IT DRP to ensure its relevance.

## 8.2 Post-Incident Review

Explain the process for conducting post-incident reviews to identify lessons learned and areas for improvement.

# 9. Appendices

## 9.1 IT Staff Contact Information

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Address** | **Phone** | **Personal Email** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 9.2 Vendor Contact Information

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Service Provided** | **Name** | **Address** | **Main Contact** | **Phone** | **Email** | **Who makes contact** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## 9.3 IT Hardware listing

|  |  |  |  |
| --- | --- | --- | --- |
| **What**Server, Laptop, Printer, Switch, Firewall, etc. | **Purpose** | **Make Model** | **Quantity** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 9.4 Network Diagram

A diagram showing the layout of the IT Infrastructure and how it is currently connected.

## 9.5 Document Revision History

Maintain a record of document revisions, including dates and descriptions of changes.

## 9.6 Glossary of Terms

Define any specialised IT terms or acronyms used in the document.

This template provides a structured framework for creating a comprehensive IT Disaster Recovery Plan (DRP) tailored to your organisation's needs. Customise the content within each section to match your specific IT environment and requirements.