[Company Name & Logo]

**Disaster Recovery Plan**

|  |  |
| --- | --- |
| Version Control | |
| Version |  |
| Author |  |
| Last Date of update |  |
| Approved by |  |

Contents

[1. Disaster Recovery Procedures 3](#_Toc193793144)

[Scope 3](#_Toc193793145)

[2. Disaster Recovery Objectives 3](#_Toc193793146)

[3. Roles and Responsibilities 3](#_Toc193793147)

[4. Key Recovery Prioritization 4](#_Toc193793148)

[5. Disaster Scenarios Covered 4](#_Toc193793149)

[6. Disaster Recovery Procedures 4](#_Toc193793150)

[7. Backup and Recovery Plan 5](#_Toc193793151)

[8. Disaster Recovery Site 5](#_Toc193793152)

[9. Appendix 5](#_Toc193793153)

# 1. Disaster Recovery Procedures

The purpose of the **Disaster Recovery Procedures** is to ensure swift restoration of critical IT systems and infrastructure following any disaster or disruption. This is a crucial component of our Business Continuity Plan, which aims to mitigate the impact of IT failures on business operations.

**Scope**

* **Included Systems**: [List the critical systems covered in this DRP]
* **Excluded Systems**: [List any systems not covered]

# 2. Disaster Recovery Objectives

* Objective 1: Minimize downtime and data loss.
* Objective 2: Ensure timely recovery of IT systems and business operations.
* Objective 3: Define roles and responsibilities for recovery efforts.

# 3. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibilities |
| Disaster Recovery Manager | Coordinates the disaster recovery process and communicates with all teams. |
| IT Infrastructure Lead | Manages recovery of hardware, networking, and data center operations. |
| Database Administrator | Restores database systems and verifies data integrity. |
| Cybersecurity Lead | Ensures that recovery processes do not compromise system security. |

# 4. Key Recovery Prioritization

|  |  |  |  |
| --- | --- | --- | --- |
| System/Service | Priority | Recovery Time Objective (RTO) | Recovery Strategy |
| [System Name] | [High/Medium/Low] | [1 hour/2 hours/4 hours] | [Backup strategy/process] |
| [System Name] | [High/Medium/Low] | [1 hour/2 hours/4 hours] | [Backup strategy/process] |
| [System Name] | [High/Medium/Low] | [1 hour/2 hours/4 hours] | [Backup strategy/process] |

# 5. Disaster Scenarios Covered

* **Natural Disasters**: [List]
* **Cyber Attacks**: [List]
* **System Failures**: [List]

# 6. Disaster Recovery Procedures

* **Step 1**: Activate the Disaster Recovery Team [Team/Person Responsible]
* **Step 2**: Assess the situation and determine the severity [Assessment Process]
* **Step 3**: Implement data backup and recovery procedures [Backup Method]
* **Step 4**: Restore IT systems to operational status [System/IT Lead]
* **Step 5**: Communicate recovery status to stakeholders [Communication Lead/Process]

# 7. Backup and Recovery Plan

* **Backup Frequency**: [Daily/Weekly]
* **Backup Locations**: [Onsite/Offsite/Cloud]
* **Data Recovery Procedure**: [Steps for recovering data]

# 8. Disaster Recovery Site

Define the location where recovery operations will take place in case the primary site is unavailable.

* **Primary Recovery Site**: [Address/Details]
* **Backup Recovery Site**: [Address/Details]

**Disaster Recovery Manager**: [Phone/Email]

**IT Lead**: [Phone/Email]

**Vendors and External Partners**: [Phone/Email]

# 9. Appendix

Include any additional resources or documents that support the DRP.

* **Appendix A**: Data Center Recovery Procedures
* **Appendix B**: Critical Systems List
* **Appendix C**: Vendor Contacts