SynrgiseLearn

Disaster Recovery Plan

Document Reference	**[Insert Reference]**
Version	1.0
Effective Date	January 03, 2025
Prepared By	Xenothan Hojem
Confidentiality Level	Confidential

Document Control Information

Version History	**Date**	**Author**	**Change Description**
Version 1.0	January 03, 2025	Xenothan Hojem	Initial Document

Organization Information:

Department	**Contact Information**
Executive	info@synrgise.com

Table of Contents

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:**
  - SynrgiseLearn SaaS platform
  - Database systems hosted on Xneelo and Vultr
  - Networking and connectivity infrastructure
  - Backup storage systems
- **Excluded Systems:**
  - Non-core business applications
  - Employee personal devices

2. Disaster Recovery Objectives

Objective 1: Minimize downtime and data loss.

Objective 2: Ensure timely recovery of IT systems and business operations within the defined RTO and RPO.

Objective 3: Define roles and responsibilities for recovery efforts.

Recovery Time Objective (RTO): 4 hours
Recovery Point Objective (RPO): 24 hours

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
Application Services	High	4 Hours	Failover to Vultr DR site
Database Systems	High	4 hours	Automated synchronization
Networking	Medium	8 hours	Redundant connectivity

5. Disaster Scenarios Covered

Synrgise's DRP covers multiple potential disaster scenarios, ensuring a comprehensive approach to maintaining business continuity. These scenarios include:

- **Natural Disasters:**
  - Earthquakes, floods, fires, and other environmental hazards that may physically damage data centers and infrastructure.
  - Mitigation Strategy: Ensure geographical redundancy, offsite backups, and tested emergency response plans.
- **Cyber Attacks:**
  - Ransomware attacks, phishing scams, and denial-of-service attacks aimed at disrupting operations or stealing sensitive data.
  - Mitigation Strategy: Regular penetration testing, endpoint protection, firewall configurations, and incident response planning.
- **System Failures:**
  - Hardware failures, software bugs, or configuration errors causing unplanned downtime.
  - Mitigation Strategy: Regular system health checks, proactive monitoring, and rapid failover mechanisms.
- **Data Corruption:**
  - Unintended data modifications, software glitches, or human errors leading to integrity issues.
  - Mitigation Strategy: Implement strict access controls, version-controlled backups, and continuous data validation procedures.
- **Human Errors:**
  - Accidental deletions, misconfigurations, or improper handling of critical systems.
  - Mitigation Strategy: Staff training, access restrictions, and detailed operational documentation.

6. Disaster Recovery Procedures

Step 1: Activate the Disaster Recovery Team (Disaster Recovery Manager)

- Notify relevant personnel
- Assess initial impact

Step 2: Assess the situation and determine severity

- Identify affected systems
- Estimate recovery efforts

Step 3: Implement backup and recovery procedures

- Initiate failover processes
- Restore from latest backups

Step 4: Restore IT systems to operational status

- Validate integrity of restored systems
- Notify stakeholders

Step 5: Communicate recovery status to stakeholders

- Provide periodic updates
- Ensure post-recovery assessment

7. Backup and Recovery Plan

Backup Frequency:

- Daily backups with 30-day retention
- Weekly backups with 52-week retention
- Monthly backups with 24-month retention

Backup Locations:

- Primary: Xneelo Datacenter
- Secondary: Vultr Johannesburg
- Offsite: Secure cloud storage

Data Recovery Procedure:

- Automated scripts verify backup integrity
- Recovery tests conducted quarterly

8. Disaster Recovery Site

Primary Recovery Site:
Xneelo Datacenter, South Africa

Backup Recovery Site:
SynrgiseLearn Offices, Johannesburg, South Africa

Contact Information:

- Disaster Recovery Manager: info@synrgise.com
- IT Lead: support@synrgise.com
- Vendors and External Partners: available on request

9. Appendix

Include any additional resources or documents that support the DRP.

- **Appendix A**: Synrgise DRS strategy