Information Technology Disaster Recovery Plan (IT DRP)

Company: Recognise Design Limited
Last Reviewed & Tested: 18/05/2026
Company Number: 08633423
Website: Recognise Design

---

1. Introduction

This document outlines the disaster recovery policies and procedures for Recognise Design Limited in the event of disruption to critical IT services, systems, infrastructure, or data.

The objective of this plan is to ensure:

- Information system availability
- Data integrity and recoverability
- Business continuity
- Minimal operational disruption

The procedures within this document are designed to support recovery within agreed recovery objectives and timeframes.

---

2. Purpose of Policy

Recognise Design Limited is committed to implementing appropriate continuity and recovery planning across all critical infrastructure, systems, and networks.

The company will:

- Maintain continuity and recovery procedures
- Periodically test recovery plans
- Ensure staff understand their responsibilities
- Keep recovery documentation updated
- Support rapid restoration of business operations

---

3. Prepared Disaster Recovery Procedures

Depending on the incident type, one or more of the following recovery procedures may be activated:

3.1 Ransomware Recovery Plan

Risks

- Malware infection
- Data encryption
- Network compromise

Systems at Risk

- Storage systems
- Employee laptops
- Shared infrastructure

Potential Impact

- Corrupted or inaccessible data
- Operational downtime

Preventative Measures

- VPN usage for remote employees
- Backup isolation
- Security patching
- User cybersecurity awareness training

Recovery Actions

- Disconnect affected systems immediately
- Do not pay ransom demands
- Validate backup availability
- Contact Abel immediately for recovery guidance
- Follow documented recovery instructions

Key Contacts

- Jordan
- Abel

3.2 Virtualised Systems Recovery Plan

Risks

- Deleted virtual machines
- VMFS corruption
- Failed backups
- RAID failures

- Corrupt guest operating systems

Systems at Risk

- Virtual machine infrastructure
- Datastores
- Hypervisor environments

Potential Impact

- Lost or corrupted virtual environments

Recovery Actions

- Restore to secondary systems where possible
- Avoid running FSCK or CHKDSK without verified backups
- Maintain updated backup procedures
- Escalate immediately to recovery specialists if required

Key Contacts

- Jordan
- Abel

3.3 RAID System Recovery Plan

Risks

- Power failures
- RAID rebuild failures
- Mechanical disk failures
- Human error
- Natural disasters

Systems at Risk

- RAID storage arrays
- Shared file systems

Potential Impact

- Complete RAID failure
- Permanent data loss

Recovery Actions

- Never run CHKDSK on damaged RAID volumes
- Label drives before removal
- Avoid repeated rebuild attempts
- Power down failing systems immediately

Key Contacts

- Jordan
- Abel

3.4 Single HDD / SSD Recovery Plan

Risks

- Mechanical drive failure
- Logical corruption
- Accidental deletion
- Reformatting

Systems at Risk

- Local workstation storage

- Standalone drives

Potential Impact

- Loss of locally stored data

Recovery Actions

- Power off immediately if hardware noises occur
- Do not dry water-damaged drives
- Use approved recovery tools where appropriate
- Escalate severe failures immediately

Key Contacts

- Jordan
- Abel

---

4. Business Impact Analysis

Business Process	Availability Target	RTO	RPO	Data Integrity	Confidentiality
IT System A	99.7%	4h	10 m	Very High	Low
IT System B	99.5%	24h	24h	Very High	High
IT System C	99.5%	48h	24h	Very High	Very High
Email System	99.5%	4h	12h	Very High	Medium

Definitions

RTO (Recovery Time Objective)
Maximum acceptable downtime before operations must resume.

RPO (Recovery Point Objective)
Maximum acceptable amount of data loss measured in time.

---

5. Robustness Analysis & Improvement Actions

Action	Description	Target Date
Backup Solution Review	Improve RPO for IT System A	18/05/2026
Email Recovery Improvements	Review shorter RTO options with supplier	18/05/2026
Secure Disk Disposal	Implement secure erase process for replaced drives	18/05/2026

---

6. Recovery Planning Procedures

General Recovery Principles

- Verify backups before changes
- Isolate affected systems
- Avoid further rebuild attempts after failure

- Maintain offsite backups using 3-2-1 strategy
- Patch systems regularly
- Provide cybersecurity awareness training

---

7. Key Personnel Contact Details

Name	Role	Contact Methods
Jordan	Director	Work / Mobile / Email
Abel	Technical Lead	Work / Mobile / Email

---

8. Revision History

Version	Date	Details
1.0	18/05/2026	Initial Version
