PLAN

Disaster Recovery Plan

Technical runbook and governance steps for major platform recovery

DOCUMENT TYPE	Plan
VERSION	1.0 · Effective 12 December 2025
OWNER	Remote-I Ltd — Technical Lead
CLASSIFICATION	Internal / Customer Assurance
REVIEW CYCLE	Annual, and after major incident or restoration exercise

ORGANISATION

LEGAL ENTITY	Remote-I Ltd
COMPANY NUMBER	15293974
REGISTERED OFFICE	45 Fitzroy Street, 4th Floor, Silverstream House, London, England, W1T 6EB
COMPLIANCE CONTACT	compliance@remote-i.com
DATA PROTECTION LEAD	Remote-I Ltd — Data Protection Lead

1. Purpose

This Disaster Recovery Plan (DRP) provides the technical runbook and governance steps required to restore the Remote-I Platform following a major incident, including service outages, data corruption, or security compromise.

2. DR Triggers and Scenarios

This DRP may be activated for:

- complete platform unavailability (hosting outage);
- database corruption or loss;
- accidental deletion of critical data;
- confirmed security breach requiring rebuild;
- destructive malware impact on server environment.

Activation is authorised by the Technical Lead or Incident Manager.

3. Assumptions and Dependencies

Key dependencies:

- hosting provider availability and provisioning tools;
- DNS control and domain management access;
- database service availability;
- secure access to configuration and secrets;
- access to backup archives and restore credentials.

Assumptions:

- backups are available in at least one recovery location;
- Customer contacts are reachable via compliance email channels.

4. Recovery Objectives

> **Baseline objectives (unless overridden by Order Form): RTO: 2–4 hours (platform restored to operational access). RPO: 24 hours (data restored to last daily backup).**

5. DR Roles

- **Incident Manager:** coordinates DR execution.
- **Technical Lead:** approves restoration decisions, security controls, and post-incident sign-off.
- **Customer Liaison:** communicates status and coordinates validation with Customer.

6. DR Runbook (Step-by-Step)

Step 1 — Declare Disaster and Stabilise

- confirm incident severity and scope;
- if security-related, preserve evidence and rotate credentials as required;
- freeze non-essential changes and restrict admin access to recovery personnel.

Step 2 — Provision Recovery Environment

- create clean hosting instance / environment;
- apply baseline hardening (permissions, HTTPS / TLS, access restrictions);
- install required runtime and cron environment.

Step 3 — Restore Application

- deploy application code from trusted source or application backup archive;
- verify file integrity and permissions;
- apply secure configuration and secrets from protected storage.

Step 4 — Restore Database

- select required restore point and verify archive integrity;
- import database dump to recovery database;
- run schema and integrity checks.

Step 5 — Restore Uploaded Files

- restore uploads and SOP files to correct storage location;
- enforce ownership and permissions;
- validate that access controls are preserved.

Step 6 — Validate Service

- authentication (including MFA for privileged roles);
- job lifecycle workflows;
- SOP access and sign-off records;
- incident workflows;
- audit log continuity;
- notification sending (email / SMS) where enabled;
- export functions where enabled.

Step 7 — Resume Operations and Monitor

- re-enable scheduled cron tasks;
- monitor logs for abnormal errors;
- confirm customer-facing availability.

Step 8 — Post Incident Review

- RCA and improvement actions;
- update risk register;
- produce report for Customers as required.

7. Evidence and Records

Remote-I maintains records of:

- DR activation decision and timeline;
- backup selection and restoration steps;
- validation test results;
- credential rotations and access changes;
- post-incident RCA and corrective actions.

8. DR Testing

A DR restore test should be performed at least every 6–12 months for production deployments, and after major releases affecting authentication, data schema, or file storage.

End of Disaster Recovery Plan. For enquiries, contact compliance@remote-i.com.