Remote–I

Business Continuity Plan (BCP)

Document Type: Plan

Version: 1.0 **Effective Date:** 12 December 2025

Owner: Remote-I Ltd – Technical Lead

Classification: Internal / Customer Assurance

Review Cycle: Annual, and after major incident or platform change

Organisation: 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 and Objectives

This Business Continuity Plan (BCP) describes how Remote-I will sustain critical service delivery during disruptive events.
The objective is to protect continuity of workforce operations, governance evidence, and platform access during pilot and production operations.

2. Scope

This plan covers continuity of:
- Platform access and authentication;
- job workflow lifecycle and scheduling functions;
- SOP distribution and sign-off workflows;
- incident reporting and governance evidence;
- audit log integrity and availability;
- backup operations and restoration capability.

This plan does not replace Customer clinical governance procedures; it supports operational continuity of the Platform.

3. Business Impact Analysis (BIA) Summary

Critical services and impact tolerances:
- Authentication and authorisation: outage prevents all use (high impact).
- Job workflows: outage disrupts staffing operations (high impact).
- SOP access/sign-off: outage reduces governance assurance (high impact).
- Incident reporting: outage reduces governance visibility (medium-high impact).
- Notifications: outage may delay communications (medium impact).

Baseline targets:
- RTO: 2–4 hours.
- RPO: up to 24 hours.

4. Continuity Strategies

Remote-I uses layered continuity strategies: A)
Technical:
- daily backups of DB and file storage;
- documented restore runbooks;
- least privilege access and segregated secrets to reduce compromise risk;
- change management to reduce instability from releases.

B) Operational:
- named incident/BCP roles (Incident Manager, Communications, Technical Lead);
- communication templates for Customers; • prioritised support triage during disruptions.

C) Supplier/hosting:
- supplier management and escalation paths;
- defined rebuild procedures for hosting failure

5. Continuity Roles and Responsibilities

- BCP Owner (Technical Lead): plan maintenance and test scheduling.
- Incident Manager: during incidents, coordinates triage, containment and recovery.
- Communications Lead: sends status updates to Customer contacts.
- Customer Contact: receives notifications and coordinates local mitigations (manual scheduling, etc.).

6. Continuity Procedures (High-Level)

During disruption:

1. Detect and declare incident; classify severity (S1–S4).
2. Communicate status to Customers based on severity and contractual obligations.
3. Identify immediate workarounds (e.g., manual scheduling fallback) and communicate guidance.
4. Restore service using DRP if required.
5. Validate service integrity and confirm normal operations.
6. Document incident, update risk register and implement improvements.

7. Communication Plan

Remote■I maintains communication principles:
- initial acknowledgement quickly for critical incidents;
- regular updates at agreed intervals for S1/S2 events;
- post■incident report provided to Customer on request (scope, timeline, lessons learned).

Communication channels:
- email to designated Customer contacts;
- status page or agreed alternative (where configured).

8. Exercising and Review

BCP exercises are recommended at least annually, including:
- tabletop scenario review (hosting outage, credential compromise, corrupted data);
- restore validation test from backups;
- verification of contact list accuracy.

Outputs:
- exercise report;
- improvement actions tracked to completion.