Remote–I

Backup & Restore Policy

Document Type: Policy

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

Owner: Remote-I Ltd – Technical Lead

Classification: Internal / Customer Assurance

Review Cycle: Annual, and after major storage/schema change or incident

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

This Backup & Restore Policy defines how Remote‑I protects the availability and integrity of Platform data through scheduled backups, controlled retention, and tested restoration procedures.
It is designed to support Customer governance, NHS DSP Toolkit expectations for recovery and resilience, and ISO/IEC 27001 operational controls.

2. Scope

This policy covers backups and restoration of:
- Platform databases (including job records, audit events, SOP acknowledgements, incident records and user accounts);
- Uploaded files (e.g., compliance documentation and SOP files stored by the Customer);
- Application code/configuration archives (where used for disaster recovery);
- Backup logs and verification evidence.

This policy applies to Pilot, staging and production environments, with stricter requirements for production.

3. Backup Objectives (RPO/RTO)

Remote‑I uses recovery objectives aligned to healthcare operational needs:
- Recovery Point Objective (RPO): up to 24 hours (daily backups), unless a customer-specific requirementis agreed.
- Recovery Time Objective (RTO): 2–4 hours for environment restore under normal conditions, subject to hosting constraints and incident complexity.

4. Roles and Responsibilities

- Technical Lead (System Owner): accountability for backup architecture, retention settings and restore testing.
- Operations/Support: monitoring backup success, handling restore requests, documenting evidence.
- Customer Administrators: request restores, validate recovered data, manage local governance communications.

5. Backup Scope and Frequency

Backup sets:
A) Database backup: scheduled daily (e.g., MySQL dump), including schema and data.
B) File backup: scheduled daily, including uploaded files and relevant storage directories.
C) Application backup: scheduled daily/weekly as appropriate, including application code required for rebuild (optional where deployment automation exists).

Backups are named with timestamped, immutable filenames to preserve chain-of-history.

6. Storage Location and Access Controls

Backups are stored outside public web roots and are not directly web-accessible. Controls include:
- restrictive directory permissions (principle of least privilege);
- access limited to operational accounts and authorised personnel;
- segregation from the live application directories where feasible;
- avoidance of storing plaintext credentials inside backup archives.

Where Customer requires additional hardening (e.g., off-site encrypted backups), this is documented and implemented via an Order Form/Security Addendum.

7. Retention and Rotation

Default retention (baseline):
• daily backups retained for 30 days;
• older backups are rotated and securely deleted after expiry.

Retention may be increased to support governance requirements, legal holds, or incident investigations.

8. Backup Verification and Evidence

Remote-I verifies backups using a combination of:
• file existence checks (timestamp, naming convention);
• file size sanity checks (non-empty, within expected range);
• automated exit-code checks of backup scripts;
• periodic restore tests into a non-production environment.

Evidence retained:
• backup execution logs (success/failure);
• restore test records and outcomes;
• incident tickets related to backup failures and corrective actions.

9. Restore Procedures (Runbook Summary)

A) Database restore:
1. Identify required restore point and archive file.
2. Verify integrity (checksum/size).
3. Extract the archive (e.g., gun zip).
4. Import to target database with controlled credentials.
5. Validate schema integrity and key workflow queries.

B) File restore:
1. Identify required file archive.
2. Extract to a safe staging location.
3. Restore required directories with correct ownership and permissions.
4. Validate access controls and file integrity.

C) Application restores (if required):
1. Deploy clean environment.
2. Restore application archive or redeploy via source/deployment pipeline.
3. Reapply secrets/configuration from secure storage.
4. Perform smoke tests and security checks.

10. Backup Failures and Escalation

If a backup fails:
• classify as operational incident;
• investigate root cause (disk space, credentials, script error, permissions);
• re-run backup after remediation;
• escalate to the Technical Lead if failure affects RPO, or if repeated failures occur;
• notify Customer if requested restore points are impacted.

11. Review and Testing

This policy is reviewed annually and after material platform changes.
Restore testing is recommended at least every 6 months for production environments, and after major schema or storage changes.

Appendix A — Restore Validation Checklist

Minimum validation after restore:
• authentication works (including MFA for privileged roles);
• job lifecycle (create/assign/accept/complete/handover);
• SOP access and SOP sign-off records present;
• incident creation and reporting views;
• audit logs show expected history;
• notification sending (email/SMS) operates (where enabled);
• exports operate (CSV/XLS/ICS) where enabled.