# Remote–I

## Logging & Monitoring 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, or after material change/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 Logging & Monitoring Policy defines the logging, retention, access, and monitoring controls used to detect issues, support investigations, and provide governance evidence. It is designed to support NHS DSP Toolkit and ISO/IEC 27001 expectations for auditability and security event monitoring.

## 2. Scope

Applies to:

- application audit logs (business and security events);
- authentication logs (login success/failure, MFA events);
- administrative and configuration change logs;
- operational logs (system errors, cron events, backup success/failure);
- (where enabled) notification delivery logs (email/SMS send attempts).

## 3. Logging Principles

Remote-I logging follows:

- minimum necessary: avoid logging sensitive content where not required (e.g., SMS message bodies);
- integrity: logs must be protected from unauthorised modification;
- availability: logs must be available for investigations and governance;
- time accuracy: logs should include reliable timestamps (UTC recommended) and consistent time source.

## 4. Event Coverage and Log Sources

The Platform should record, at minimum:

- user authentication events (login attempts, password resets, MFA enrolment);
- role and privilege changes;
- job lifecycle transitions (created/assigned/accepted/in progress/completed/handover);
- SOP publishing and SOP acknowledgements/signatures;
- incident creation and updates;
- export/report generation actions;
- backup execution results (success/failure);
- security relevant errors or anomalies.

Where available, logs include user ID, role, IP address (or equivalent), timestamp, and event type.

## 5. Log Access and Protection

- Access to logs is restricted to authorised personnel.
- Customer administrators may access governance logs relevant to their organisation.
- Remote-I operational personnel may access logs necessary for support and security, subject to confidentiality obligations.
- Logs must not be stored in publicly accessible directories.

## 6. Retention and Disposal

Retention is risk-based and must support governance and investigations. Typical baseline:
• audit logs: 12 months (configurable);
• security/auth logs: 12 months;
• operational logs: 3–12 months depending on volume;
• backups: per backup policy (e.g., 30 days).

At expiry, logs are deleted/rotated securely. Retention may be extended for legal holds or active investigations.

## 7. Monitoring and Alerting

Remote-I monitors for:
• repeated failed logins or suspicious access patterns;
• privilege escalations;
• abnormal export activity;
• backup failures;
• unexpected spikes in errors or system resource anomalies.

Alerting thresholds should be reviewed periodically and tuned to reduce false positives.

## 8. Incident Support and Evidence Handling

Logs are used as evidence during incidents. Requirements:
• preserve relevant logs for incident time windows;
• maintain chain-of-custody where required;
• limit access to incident logs to need-to-know personnel;
• ensure incident findings feed into corrective actions and risk register updates.

## 9. Privacy and Transparency

Logging is conducted for legitimate security and governance purposes. Remote-I and Customers should ensure that users are informed via privacy notices and acceptable use policies.