Remote– I

Supplier & Subprocessor Management 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 Supplier & Subprocessor Policy defines how Remote‑I selects, contracts with, monitors, and offboards third‑party suppliers and subprocessors that may affect security, privacy, and service continuity. It supports NHS DSP Toolkit supplier governance expectations and ISO/IEC 27001 requirements for supplier relationship management.

2. Scope

Applies to all third parties who:
- host or process Customer Data;
- provide communications services (email/SMS);
- provide operational tooling that interfaces with production;
- provide professional services with privileged access (support, development, security testing).

3. Supplier Risk Classification

Suppliers are risk-rated based on:
- access to Customer Data or credentials;
- criticality to service availability;
- geographic location and international transfer implications;
- security maturity and contractual assurances.

Typical tiers:
- Tier 1: processes Customer Data or provides core hosting.
- Tier 2: supports communications or operational monitoring with limited data.
- Tier 3: non-critical suppliers with no access to Customer Data.

4. Due Diligence and Onboarding

Before onboarding Tier 1/2 suppliers, Remote‑I performs due diligence proportionate to risk, which may include:
- security questionnaire and review of controls;
- review of data location and transfer mechanisms;
- review of certifications or independent assurance (where available);
- contractual review for confidentiality, breach notification, and subprocessing restrictions;
- assessment of resilience (backup, DR, uptime practices).

All suppliers must be contractually bound to confidentiality obligations.

5. Contractual Requirements

Contracts with suppliers/subprocessors must include (as applicable):

- data processing terms (Article 28 equivalent where supplier is a Processor);
- breach notification timelines;
- access restrictions and least privilege;
- audit and assurance rights (directly or via reports);
- termination support and secure deletion obligations;
- restrictions on further subprocessing without approval.

6. Ongoing Monitoring

Remote-I periodically reassesses Tier 1 suppliers (at least annually) and reassesses suppliers after:

- major incidents;
- changes in ownership;
- changes in data location;
- material service changes.

Supplier performance and incidents are documented and feed into risk management.

7. Subprocessor List and Customer Notification

Remote-I maintains a current list of subprocessors used to deliver the Platform. Customers are notified of material changes as set out in the DPA and may object on legitimate grounds.

8. Offboarding and Exit

When a supplier relationship ends:

- access is revoked immediately;
- credentials and keys are rotated where applicable;
- data return/deletion is confirmed in writing;
- exit risks are assessed and mitigated.