Remote–I

Information Security 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 Information Security Policy establishes the security governance framework for the Remote-I Platform and the Remote-I organisation.
It defines mandatory security principles, responsibilities, and control requirements to protect confidentiality, integrity and availability of information processed by Remote-I.

This policy is designed to support evidence requirements commonly assessed during NHS DSP Toolkit reviews, ISO/IEC 27001 supplier assurance, hospital procurement due diligence, grant evaluations, and enterprise partner security assessments.

2. Scope

This Policy applies to:

- the Remote-I Platform (application code, databases, storage, backups, logs, and operational tooling);
- Remote-I personnel and contractors with access to production systems;
- Customer administrators and authorised users as applicable to their use of the Platform; and
- third-party suppliers and sub processors that support service delivery.

The policy covers information processed within the Platform, including workforce metadata, compliance documentation, SOP acknowledgements, job lifecycle data, incident records, audit logs, and operational security telemetry.

3. Security Objectives and Principles

Remote-I follows these baseline principles:

- Least privilege: access is granted only to the minimum required for a role.
- Defence in depth: multiple layers of protection across identity, application, infrastructure, and monitoring.
- Security by design and default: controls are embedded into architecture, not added after the fact.
- Accountability and traceability: security relevant actions are logged and reviewable.
- Data minimisation: the Platform is designed to avoid unnecessary processing of patient identifiable clinical data.
- Resilience: backups and recovery processes support continuity and rapid restoration.

Primary objectives:
A) protect Customer Data and system credentials from unauthorised access; B)
maintain data integrity of governance records (e.g., SOP sign-off, audit trails);
C) ensure service availability consistent with contractual commitments.

4. Governance and Roles

Remote-I assigns security responsibilities as follows:

- Executive accountability: Remote-I leadership retains ultimate accountability for information security.
- Data Protection Lead: oversees privacy governance, DPIAs, and data protection obligations.
- Technical Lead / System Owner: responsible for security architecture, patching, configuration, and access control enforcement.
- Incident Manager (may be same as Technical Lead): coordinates security incident response and communications.

All personnel with system access must complete security onboarding and adhere to confidentiality obligations.

5. Risk Management

Remote-I maintains a risk based security approach:

- Identify assets and threats (including credential compromise, data leakage, service outages).
- Assess likelihood and impact, including regulatory and reputational impact.
- Implement controls proportionate to risk.
- Review risks after significant changes, incidents, or supplier updates.

Risk artefacts may include: risk register, change records, DPIA outputs, incident reports, and supplier assessments.

6. Asset Management and Data Classification

Remote-I maintains an inventory of key information assets (e.g., databases, backup archives, uploaded files, audit logs, configuration secrets).
Data is classified according to sensitivity, typically:

- Public: marketing and website content.
- Internal: operational procedures, nonsensitive internal documentation.
- Confidential: customer operational data, workforce compliance documents, audit logs.
- Restricted: credentials/secrets, security incident details, high sensitivity governance records.

Classification determines access control, retention, and handling requirements.

7. Access Control

Access is managed via:

- role based access control (RBAC) at the application layer;
- separation of roles between Customer administrators and radiographers;
- strong authentication requirements, including MFA support for privileged accounts;
- controlled administrative access to hosting and production systems (restricted to named personnel).

Details are defined in the Access Control & MFA Policy.

8. Secure Configuration and Secret Management

Remote-I requires:

- secrets (API keys, SMTP credentials, database credentials) to be stored outside public web roots andprotected by restrictive permissions;
- separation between application code and configuration;
- prohibition of hardcoding secrets into publicly accessible files or repositories; • periodic credential rotation, especially after suspected exposure or personnel changes.

Configuration changes are subject to change management controls.

9. Cryptography and Encryption

Remote-I mandates:
- encryption in transit using HTTPS/TLS for Platform access;
- secure email transport where supported by provider (TLS);
- encryption and/or access restrictions for backup archives and stored files consistent with hosting capabilities and risk profile;
- avoidance of weak or deprecated cipher suites where configurable.

Where Customer requires specific cryptographic standards, these may be documented in an Order Form/Security Addendum.

10. Logging, Monitoring and Auditability

Remote-I maintains audit logs covering:
- authentication events;
- privilege changes and administrative actions;
- job lifecycle state transitions;
- SOP acknowledgements/sign offs;
- incident record creation and updates.

Logs are protected from unauthorised modification and are retained in line with governance requirements. Monitoring and alerting principles are defined in the Logging & Monitoring Policy.

11. Vulnerability and Patch Management

Remote-I maintains a patch and vulnerability management program:
- regular patch cycles for server and application dependencies;
- prioritised remediation for critical vulnerabilities;
- documented emergency patch processes;
- verification testing and rollback planning.

Details are defined in the Vulnerability & Patch Management Policy.

12. Supplier and Subprocessor Security

Remote-I evaluates suppliers based on:
- data access scope and data location;
- security posture and controls;
- contractual protections (confidentiality, breach notification, subprocessing restrictions);
- operational resilience.

Supplier governance is defined in the Supplier & Subprocessor Policy.

13. Incident Management

Remote-I maintains an incident response process to:
• detect and triage security events;
• contain and eradicate threats;
• restore service and data integrity;
• notify Customers as required by contract and data protection law;
• perform root cause analysis and improvement actions.

Details are defined in the Incident Response Policy.

14. Training and Awareness

Remote-I personnel with production access must:
• complete security onboarding (including credential handling, phishing awareness, incident reporting);
• follow documented procedures for access and changes;
• participate in periodic refreshers and tabletop incident exercises where applicable.

15. Review and Exceptions

This policy is reviewed at least annually, and additionally after material security incidents or significant platform changes.
Exceptions require written approval by the Technical Lead and must include compensating controls and an expiry date.