Remote–I

Incident Response 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 Incident Response Policy defines how Remote-I detects, manages, and resolves security incidents, including personal data breaches, in a controlled and auditable manner.
It supports Customer governance requirements, NHS DSP Toolkit expectations, and ISO/IEC 27001 incident management control objectives.

2. Scope

Applies to:
- security incidents affecting the Platform, infrastructure, or Customer Data;
- suspected credential compromise or unauthorised access;
- malware or exploitation attempts;
- data integrity incidents affecting audit logs or governance records;
- personal data breaches under UK GDPR/GDPR.

3. Definitions

- Security Incident: any event that compromises (or may compromise) confidentiality, integrity, oravailability.
- Personal Data Breach: a breach of security leading to accidental or unlawful destruction, loss, alteration,unauthorised disclosure of, or access to Personal Data. • Severity: classification used to prioritise response (S1–S4).

4. Roles and Responsibilities

- Incident Manager: coordinates technical response, containment, eradication, and recovery.
- Data Protection Lead: assesses breach notification obligations and coordinates privacy communications.
- Communications Lead (as applicable): manages external communications with Customers and partners.
- Customer Contact: designated contact for notifications under the contract/DPA.

5. Severity Classification

Remote-I uses the following baseline severity model:
- S1 (Critical): active compromise, major outage, or high likelihood of personal data exposure.
- S2 (High): significant impairment, confirmed suspicious access, limited scope.
- S3 (Medium): contained issue with limited impact.
- S4 (Low): minor issue, no evidence of compromise, monitoring only.

Severity determines response urgency and escalation.

6. Incident Response Lifecycle

A) Detection and Reporting
- incidents may be detected via monitoring, customer reports, or internal review.
- all staff must report suspected incidents immediately to the Incident Manager.

B) Triage and Containment
- confirm incident scope and affected systems.

• contain by disabling accounts, rotating keys, isolating services, blocking malicious IPs.
C) Eradication and Remediation
• remove malicious artefacts, fix vulnerabilities, apply patches.
• ensure affected credentials are rotated and access is restored safely.

D) Recovery
• restore service (including from backups if needed).
• validate platform functions and integrity of audit logs.

E) Post-Incident Review
• conduct root cause analysis (RCA).
• document corrective and preventive actions.
• update risk register and improve controls.

7. Breach Notification

Where Remote-I acts as Processor, Remote-I will notify the Customer (Controller) without undue delay upon becoming aware of a relevant Personal Data Breach, in accordance with the DPA.

Customer (Controller) remains responsible for notifying supervisory authorities and affected individuals where required, with Remote-I assistance.

8. Evidence Preservation

Remote-I preserves relevant logs and artefacts for investigation, including:
• authentication logs;
• audit trails;
• system error logs;
• configuration and change records.

Access to evidence is restricted and documented.

9. Testing and Exercises

Remote-I performs periodic incident response testing (tabletop exercises) and reviews playbooks after major incidents or significant platform changes.