Remote–I

Vulnerability & Patch 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 Vulnerability & Patch Management Policy defines how Remote-I identifies, prioritises, remediates, and verifies vulnerabilities affecting the Platform, infrastructure, and dependencies.
It supports NHS DSP Toolkit security assurance and ISO/IEC 27001 operational security expectations.

2. Scope

Applies to:
- hosting OS and server components;
- web server and runtime (e.g., PHP, libraries);
- application code and third-party packages;
- database components;
- operational tooling used for backups, notifications and monitoring.

3. Vulnerability Sources

Remote-I monitors vulnerabilities using one or more of:
- vendor security advisories;
- CVE feeds and security mailing lists;
- dependency scanning and SCA tools (where used);
- penetration test findings (where commissioned);
- internal testing and code review;
- responsible disclosure reports.

4. Severity and Remediation Targets

Remote-I prioritises remediation based on severity and exploitability. Baseline targets:
- Critical (active exploit / high impact): mitigate within 48–72 hours where feasible.
- High: mitigate within 7–14 days.
- Medium: mitigate within 30–60 days.
- Low: address in normal backlog.

Where immediate patching is not feasible, compensating controls (WAF rules, access restrictions, feature disablement) may be applied.

5. Patch Process

A) Identify and assess impact.
B) Prepare fix/patch and test in non-production where practicable.
C) Schedule deployment under Change Management controls.
D) Deploy patch and verify service health.
E) Record evidence: change record, version notes, and verification results.

6. Emergency Patching

For critical vulnerabilities, Remote-I may deploy emergency changes outside normal windows to reduce risk. Emergency changes are documented retrospectively and reviewed.

7. Verification and Rollback

All patches require:

- verification checks (functional smoke tests, security validation where relevant);
- rollback plan for production deployments;
- monitoring following release for abnormal errors or regressions.

8. Exceptions

Any exception to remediation targets requires:

- documented risk acceptance;
- compensating controls;
- approval by the Technical Lead;
- a defined expiry date.