Remote–I

Change 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

© 2025 Remote-I Ltd

1. Purpose

This Change Management Policy ensures that changes to the Remote-I Platform are planned, risk-assessed, tested, approved, and recorded to protect service stability, security, and compliance. It supports NHS DSP Toolkit governance evidence and ISO/IEC 27001 change control expectations.

2. Scope

Applies to changes affecting:
• application code, configuration, and dependencies;
• database schema changes;
• security controls and authentication settings;
• integrations (email/SMS, exports);
• infrastructure settings impacting availability or data security.

3. Change Types

• Standard Change: low risk, pre-approved, repeatable (e.g., routine configuration updates).
• Normal Change: requires assessment and approval prior to implementation.
• Emergency Change: urgent change to mitigate an active security risk or major outage.

4. Change Requirements

All changes must include:
• description and business/technical justification;
• risk assessment (security, privacy, availability);
• test plan and validation steps;
• implementation plan and timing;
• rollback plan;
• communication plan (if customer-facing).

5. Approval and Segregation of Duties

Remote-I uses proportional approvals:
• Normal changes require review by a peer or designated approver where practicable.
• High-risk changes (security/auth, data migration) require explicit Technical Lead approval.
• Emergency changes may be approved verbally or rapidly but must be documented post-implementation.

6. Testing and Release Management

• Changes should be tested in a non-production environment where feasible.
• Releases include post-deployment smoke tests.
• Monitoring should be increased temporarily following major releases.

© 2025 Remote-I Ltd

7. Change Records and Evidence

Remote-I maintains evidence including:
• change tickets or release notes;
• code review notes where applicable;
• deployment timestamps;
• rollback outcomes (if used);
• post-implementation review actions.

8. Post-Implementation Review

For significant or high-risk changes, a post-implementation review should confirm:
• objectives achieved;
• no unacceptable regressions;
• documentation updated;
• learnings captured for continuous improvement.

© 2025 Remote-I Ltd