Remote–I

Access Control & MFA 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 Access Control & MFA Policy defines mandatory requirements for user identity management, authentication, authorisation, and session security for the Remote-I Platform. It supports NHS DSP Toolkit and ISO/IEC 27001 expectations for access control, least privilege, and accountability.

2. Scope

Applies to:

- all Platform user accounts (Customer administrators, hospital users, radiographers);
- Remote-I administrative access to hosting, databases, and operational tooling;
- API keys and service accounts used for email/SMS and integrations (where applicable).

3. Access Control Principles

Remote-I enforces:

- Least privilege: access is limited to what is required for the role.
- Segregation of duties: administrative actions are separated from standard user actions.
- Default deny: new features or modules are not accessible until explicitly permitted by role.
- Accountability: significant actions must be attributable to a named account via audit logs.

4. Account Lifecycle (Joiner-Mover-Leaver)

Customer is responsible for managing Authorised Users within its organisation. Requirements:

- Joiners: accounts may be created only by authorised administrators; identity must be verified (emailverification) prior to activation.
- Movers: role changes must be recorded, and access reduced when duties change.
- Leavers: access must be revoked promptly (same day where practicable); shared accounts areprohibited.

Remote-I administrative accounts are provisioned only to named personnel and removed immediately upon offboarding.

5. Authentication Requirements

Password requirements:

- minimum length: 12 characters recommended (Customer may impose stricter rules);
- passwords must be unique and not reused across services;
- suspected compromise requires immediate reset.

MFA requirements:

- MFA is required for privileged roles (e.g., Customer administrators and Remote-I administrative access), unless explicitly disabled by Customer policy and risk acceptance.
- MFA is strongly recommended for all users with access to compliance documents, SOP modules, incident dashboards, or audit exports.
- MFA methods should be phishing resistant where feasible (TOTP acceptable for pilot use; hardware keys preferred for high assurance environments).

6. Session Security

Remote-I enforces session protections proportionate to risk:
• secure session identifiers;
• idle timeout and absolute session lifetime (configurable by Customer plan where applicable);
• session invalidation on password reset and role change;
• protection against CSRF for authenticated actions (where applicable).

Users must not share sessions or keep sessions open on shared devices.

7. Privileged Access Management (PAM)

Privileged access includes:
• managing users and roles;
• exporting audit reports;
• editing SOP libraries;
• approving compliance documents; • administrative configuration changes.

Requirements:
• privileged actions must be logged (who/what/when).
• privilege assignment must be reviewed periodically (at least quarterly for production deployments).
• administrative access to hosting must be limited to Remote-I operational personnel and protected by MFA/keys where supported.

8. Access Reviews

Customer administrators should perform periodic access reviews to ensure:
• only current staff have accounts;
• roles match job functions;
• no orphaned accounts exist.

Remote-I can support access review evidence by providing audit logs and user lists where available.

9. Exceptions

Exceptions (e.g., disabling MFA for specific roles) require:
• documented rationale;
• compensating controls (e.g., network restrictions, increased monitoring);
• approval by Customer security lead and Remote-I Technical Lead (for production).

10. Enforcement

Violations may result in account suspension, forced credential resets, and incident investigation.

Remote-I may suspend access where account activity indicates compromise risk.