

Security & Compliance Overview

A plain-language summary of the security controls, tenant isolation model and compliance posture of the RiderScore platform.

Version 1.0 | Effective 19 August 2026 | Last reviewed 19 August 2026

RiderScore Technologies Ltd · riderscore.co.ke

1. Scope

This overview describes the controls in place for the RiderScore platform and APIs. It is a summary for prospective and existing customers and does not replace contractual security terms.

2. Encryption

Traffic between clients and the platform is served over TLS. Data at rest is encrypted by our managed database and storage infrastructure.

Credentials and secrets are stored in managed secret storage and are never committed to source control.

3. Tenant isolation

The organisation is the security boundary. Every rider record, score snapshot and audit entry is bound to an organisation.

Isolation is enforced in the database with row level security policies, not only in application code, so a query cannot cross a tenant boundary.

4. Access control

Access is role-based. Roles include organisation administrator, credit officer, risk analyst, fraud investigator, operations manager and read-only.

Permissions follow least privilege, and organisation administrators can grant or revoke access for their own users at any time.

5. Auditability

Sign-ins, rider lookups, score calculations, exports and administrative changes are recorded in an append-only audit log with actor, organisation and timestamp.

Score snapshots are immutable, so a decision made in the past can be reconstructed and explained.

6. Application and infrastructure security

The platform runs on managed cloud infrastructure with patching handled by the provider.

Changes are reviewed before release, dependencies are monitored for known vulnerabilities, and automated security checks run against the codebase.

7. Incident response

We maintain an incident process covering detection, triage, containment, remediation and post-incident review.

Where an incident meets the legal threshold, we notify affected parties and the relevant regulator within the timeframe required by law.

8. Vulnerability reporting

Report suspected vulnerabilities to security@riderscore.co.ke with enough detail to reproduce the issue.

Please do not access data belonging to others, degrade the service, or disclose publicly before we have had a reasonable opportunity to remediate. We will acknowledge reports and keep reporters informed.

9. Compliance posture

The platform is designed around the principles of the Kenya Data Protection Act, 2019, including lawful basis, data minimisation, purpose limitation, accuracy and data subject rights.

Statements about formal certifications or independent audits will only be published here once they have been completed and confirmed. Customers requiring assurance documentation should contact security@riderscore.co.ke.