RAILS CLOUD

Security Overview

How Rails Cloud protects your data, workloads, and infrastructure

Version	Effective Date	Classification	Review Cycle
1.0	**1 March 2026**	**Public**	**Bi-annual**

1. Our Security Philosophy

Security is not a feature at Rails Cloud — it is the foundation on which every product is built. As an infrastructure provider serving African businesses across fintech, healthcare, education, and enterprise, we understand that our customers are entrusting us with their most critical workloads and their users' most sensitive data.

Our security programme is built on three principles:

Defence in Depth	Least Privilege	Transparency
Multiple overlapping security controls so that no single failure exposes your data	Every system, user, and process has only the minimum access required to perform its function	We publish our security posture publicly and provide detailed documentation to enterprise customers on request

2. Infrastructure Security

2.1 Physical Security

Rails Cloud infrastructure runs on Amazon Web Services (AWS), with primary hosting in the AWS Cape Town region (af-south-1) for African data residency. AWS data centres maintain:

- ISO 27001 certification and SOC 1, SOC 2, and SOC 3 audit compliance
- 24/7 physical security with biometric access controls, security personnel, and CCTV
- N+1 redundancy for power and cooling with multiple utility feeds
- Geographic redundancy across multiple availability zones

Rails Cloud does not operate its own physical data centres. Physical security responsibilities are shared with AWS under the AWS Shared Responsibility Model. AWS physical security documentation is available at aws.amazon.com/security.

2.2 Network Security

All Rails Cloud production infrastructure is deployed within isolated Virtual Private Clouds (VPCs) with strict network segmentation:

Control	Implementation
Network segmentation	Production, staging, and management networks are fully isolated. No lateral movement between customer VPCs is possible.
Firewall rules	Restrictive security group rules applied at instance level. Default-deny posture — only explicitly required traffic permitted.
DDoS protection	AWS Shield Standard on all infrastructure. Shield Advanced available for Enterprise customers on request.
Intrusion detection	Network-level IDS/IPS monitoring all production traffic. Automated alerting on anomalous traffic patterns.
WAF	Web Application Firewall deployed in front of all public-facing Rails Cloud services. OWASP Top 10 rules enforced.
Private endpoints	Internal services communicate over private network endpoints only. No unnecessary public IP exposure on internal components.

2.3 Shared Responsibility Model

Rails Cloud operates a shared security responsibility model. Understanding the boundary between Rails Cloud's responsibilities and the Customer's responsibilities is essential for a secure deployment:

Rails Cloud Responsible For	Customer Responsible For
Physical and network infrastructure security	Application-level security of deployed workloads
Hypervisor and virtualisation layer	Operating system patching on customer VMs (VPS)
Managed database engine security	Database access controls and query security
Platform authentication and Rails ID	Customer account credential security and MFA adoption
Encryption at rest and in transit (platform layer)	Application-level encryption of sensitive data fields
Platform-level monitoring and incident response	Application monitoring and incident response for customer workloads
Rails Cloud employee access controls	Authorised user management within the Customer account

3. Data Security

3.1 Encryption at Rest

All data stored on Rails Cloud infrastructure is encrypted at rest using AES-256 encryption. This applies to:

- All managed database instances (PostgreSQL)
- Object storage (all buckets encrypted by default with no option to disable)

- VM disk images and snapshots
- Backup archives and offsite replicas
- Rails Pay transaction records and KYC documents

3.2 Encryption in Transit

All data transmitted between customers and Rails Cloud, and between internal Rails Cloud services, is encrypted in transit:

- TLS 1.2 minimum enforced on all public-facing endpoints — TLS 1.0 and 1.1 are disabled
- TLS 1.3 supported and preferred on all Rails Cloud APIs and dashboard
- Internal service-to-service communication encrypted via mutual TLS (mTLS) where applicable
- Certificate management automated via Let's Encrypt and AWS Certificate Manager — no manual certificate handling
- HSTS enforced on all web properties with a minimum age of 1 year

3.3 Key Management

Encryption keys are managed using AWS Key Management Service (KMS) with the following controls:

- Separate encryption keys per customer for managed database instances on Business and Enterprise tiers
- Automatic key rotation on an annual cycle
- No Rails Cloud personnel have access to plaintext customer encryption keys
- Key access audit logs maintained and available to Enterprise customers on request

3.4 Data Isolation

Customer data is logically isolated at the database, storage, and network layers. Rails Cloud's multi-tenant architecture ensures:

- No customer can access another customer's data through the platform APIs
- Managed database instances are deployed in dedicated containers — no shared database instances between customers
- Object storage buckets are scoped to individual customer accounts with strict IAM policies

4. Access Control

4.1 Internal Access Controls

Rails Cloud enforces strict internal access controls on all production systems:

Control	Detail
Role-based access control	All internal access to production systems governed by RBAC. Roles reviewed quarterly and updated on personnel changes.
Least privilege enforcement	No standing administrative access to production. Engineers use time-limited, approval-gated elevated access for specific tasks only.

Control	Detail
Multi-factor authentication	MFA mandatory for all Rails Cloud personnel with any level of production access. Hardware security keys required for privileged access.
Privileged access management	All privileged sessions recorded and logged. Jump server architecture — no direct SSH to production instances.
Access reviews	Quarterly access reviews across all production systems. Immediate revocation on personnel departure.
Separation of duties	No single engineer can both approve and deploy changes to production. Peer review required for all production modifications.

4.2 Customer Account Access Controls

Rails Cloud provides the following access control tools to customers for managing their own account security:

- Multi-factor authentication (MFA) available on all account tiers — strongly recommended and required on Enterprise
- Role-based access for team members: Owner, Admin, Developer, Billing — configurable per user
- API key scoping: keys can be restricted to specific services, IP ranges, and permission sets
- Session management: configurable session timeouts and active session visibility
- Audit logs: all account actions logged with user, timestamp, IP address, and action detail — retained 12 months
- IP allowlisting: restrict account access to specified IP ranges (Business and Enterprise tiers)

5. Vulnerability Management

5.1 Patch Management

Rails Cloud maintains a formal patch management programme with the following SLAs for applying security patches to platform infrastructure:

Severity	CVSS Score	Patch SLA	Example
Critical	9.0 – 10.0	24 hours	Remote code execution, authentication bypass
High	7.0 – 8.9	72 hours	Privilege escalation, significant data exposure
Medium	4.0 – 6.9	14 days	Information disclosure, limited exploit conditions
Low	0.1 – 3.9	90 days	Minor configuration issues, theoretical risks

5.2 Dependency Scanning

All Rails Cloud application code and infrastructure dependencies are scanned automatically on every deployment using automated software composition analysis (SCA) tools. Newly discovered vulnerabilities in existing dependencies trigger automated alerts and are prioritised according to the patch SLA schedule above.

5.3 Penetration Testing

Rails Cloud conducts periodic third-party penetration testing of the platform by independent security firms. The scope covers web application, API, network, and infrastructure layers. Summaries of the most recent penetration test findings and remediation status are available to Enterprise customers under NDA upon request to security@railscloud.co.

5.4 Responsible Disclosure

Rails Cloud operates a responsible vulnerability disclosure programme. Security researchers who discover vulnerabilities in the Rails Cloud platform are encouraged to report them to security@railscloud.co. Researchers acting in good faith will not face legal action. Full programme details are published at railscloud.co/security/disclosure.

6. Identity and Authentication

6.1 Password Security

Rails Cloud enforces the following password security controls for all user accounts:

- Minimum password length of 12 characters
- Passwords hashed using bcrypt with a per-user salt — plaintext passwords are never stored
- Compromised password detection: passwords checked against known breach databases (HaveIBeenPwned API) at registration and on change
- Account lockout after 10 consecutive failed login attempts with progressive delay

6.2 Multi-Factor Authentication

Rails Cloud supports the following MFA methods:

- Time-based one-time password (TOTP) via authenticator apps (Google Authenticator, Authy, 1Password)
- Hardware security keys (FIDO2/WebAuthn) for Enterprise accounts
- SMS OTP as a fallback method (not recommended as primary factor)

6.3 API Authentication

All Rails Cloud API access is authenticated using scoped API keys with the following security properties:

- Keys are generated with cryptographically secure randomness — 256-bit entropy minimum
- Keys are displayed only once at creation — Rails Cloud does not store recoverable copies
- Keys can be scoped to specific services, IP ranges, and HTTP methods
- Key usage is logged in real-time and visible in the account audit log
- Inactive keys (no usage in 90 days) generate automated alerts for review

7. Security Monitoring and Incident Response

7.1 Continuous Monitoring

Rails Cloud operates a 24/7 security monitoring programme across all production infrastructure:

- Centralised security information and event management (SIEM) aggregating logs from all platform components
- Automated anomaly detection for unusual access patterns, data volumes, and API usage
- Real-time alerting for security events with defined escalation paths
- Uptime and availability monitoring with sub-60-second check intervals from multiple global locations
- Network flow analysis for DDoS detection and traffic anomalies

7.2 Incident Response

Rails Cloud maintains a documented incident response plan covering detection, containment, eradication, recovery, and post-incident review. Response time commitments by incident severity are published in the Rails Cloud Service Level Agreement.

For security incidents involving Customer Data, Rails Cloud will notify affected customers within 48 hours of confirming the incident, in accordance with the Data Processing Agreement. Post-incident reports are published for all P1 and P2 incidents within 5 business days of resolution.

7.3 Audit Logging

Comprehensive audit logs are maintained across all platform layers:

- All API calls logged with endpoint, timestamp, source IP, response code, and authenticated identity
- All privileged administrative actions on production infrastructure logged with immutable audit trail
- All customer account actions (login, configuration changes, resource creation/deletion) logged and accessible via the dashboard
- Logs retained for a minimum of 12 months and stored in tamper-evident, write-once storage

8. Business Continuity and Disaster Recovery

8.1 Backup Policy

Data Type	Backup Frequency	Retention	Recovery Point Objective
Managed databases	Continuous (WAL) + daily snapshot	30 days	5 minutes (Business+)
VPS disk images	Daily snapshot	7 days (extendable)	24 hours

Data Type	Backup Frequency	Retention	Recovery Point Objective
Object storage	Versioning + cross-region replication	Configurable	Near-zero
Rails Cloud platform config	Continuous (infrastructure as code)	Indefinite (versioned)	Near-zero

8.2 Recovery Time Objectives

Rails Cloud targets the following recovery time objectives (RTOs) in the event of a platform-level failure:

- Platform infrastructure recovery: 4 hours (P1 incident)
- Managed database recovery from backup: 2 hours for Business tier, 1 hour for Enterprise tier
- Full region failover (Enterprise): as per individual enterprise agreement

8.3 Backup Testing

Rails Cloud performs quarterly backup restoration tests across all backup types. Test results are reviewed by the engineering team and any failures trigger immediate remediation. Enterprise customers may request a summary of recent backup test outcomes from enterprise@railscloud.co.

9. Personnel Security

- Background screening is conducted for all employees and contractors with access to production systems or Customer Data, in compliance with applicable Zimbabwean employment law
- All personnel with access to production systems sign confidentiality agreements prior to commencing work
- Mandatory security awareness training completed by all staff on joining and annually thereafter
- Phishing simulation exercises conducted on a regular cadence
- Access to production systems is revoked immediately on departure — automated offboarding checklist enforced
- Rails Cloud employees may not access Customer Data except where explicitly requested by the Customer for support purposes or where required for platform security operations

10. Compliance and Certifications

Standard / Framework	Status	Detail
Zimbabwe Cyber and Data Protection Act (ZDCPA)	**Implemented**	Full compliance with data protection obligations as data processor and controller
AWS Shared Responsibility Model	**Implemented**	Infrastructure layer covered by AWS ISO 27001 / SOC 2 certifications

Standard / Framework	Status	Detail
TLS 1.2+ Encryption Standards	**Implemented**	All public endpoints enforced; TLS 1.0 and 1.1 disabled platform-wide
OWASP Top 10	**Implemented**	WAF rules enforced; code security reviews align to OWASP guidelines
PCI-DSS (Rails Pay)	**In Progress**	Alignment programme underway; see Rails Pay PCI-DSS Statement
ISO 27001	**Planned**	Formal certification roadmap targeting Q4 2026
SOC 2 Type II	**Planned**	Audit readiness programme underway; targeting Q1 2027
GDPR / POPIA / NDPR	**Implemented**	DPA framework covers cross-border customer compliance obligations

11. Enterprise Security Documentation

Enterprise customers and prospects undergoing vendor security assessment may request the following documentation from security@railscloud.co:

- Infrastructure architecture diagram and data flow documentation
- Most recent third-party penetration test summary (under NDA)
- AWS SOC 2 / ISO 27001 certificates (available directly from AWS)
- Business continuity and disaster recovery plan summary
- Data residency confirmation letter
- Subprocessor list with data processing details
- Completed security questionnaires (SIG Lite, CAIQ, or custom)

ENTERPRISE	Rails Cloud's security team is available to participate in vendor security review calls, complete security questionnaires, and provide architecture walkthroughs for Enterprise prospects. Contact enterprise@railscloud.co to schedule.

12. Security Contact and Reporting

Matter	Contact	Response Time
Security incidents (active)	security@railscloud.co	4 hours (24/7)
Vulnerability disclosure	security@railscloud.co	48 hours
Enterprise security review	enterprise@railscloud.co	1 business day
Penetration test notification	security@railscloud.co	Acknowledged same day
Data breach notification	privacy@railscloud.co	48 hours (as Processor)

Matter	Contact	Response Time
General security queries	security@railscloud.co	1 business day

This Security Overview is published at railscloud.co/security and reviewed bi-annually. It is intended to provide transparency about Rails Cloud's security posture to customers, prospects, and partners. Detailed technical documentation is available to Enterprise customers under NDA. Rails Net (Private) Limited, Reg. 84172A0722026, TIN 2002425765, Zimbabwe.