RAILS CLOUD

Acceptable Use Policy

Defining responsible and lawful use of the Rails Cloud platform

Version	Effective Date	Applies To	Jurisdiction
1.0	**1 March 2026**	**All Rails Cloud Users**	**Republic of Zimbabwe**

1. Purpose and Scope

This Acceptable Use Policy ("AUP") sets out the rules governing acceptable and prohibited use of the Rails Cloud platform, including all products, services, APIs, and infrastructure provided by Rails Net (Private) Limited, trading as Rails Zimbabwe ("Rails Cloud", "we", "us").

This AUP applies to:

- All registered Customers and their Authorised Users
- All individuals accessing Rails Cloud services under a free trial or beta programme
- All workloads, applications, and data processed on or transmitted through Rails Cloud infrastructure
- Third-party developers using the Rails Cloud Developer API

This AUP is incorporated into and forms part of the Rails Cloud Terms of Service. By using Rails Cloud, you agree to comply with this AUP. Violations may result in suspension or termination of your account in accordance with the Terms of Service.

PRINCIPLE Rails Cloud is built to power African innovation. This AUP exists not to restrict legitimate use but to protect the platform, our customers, and the communities we serve from harm. When in doubt, contact us at aup@railscloud.co before proceeding.

2. General Conduct Standards

All users of the Rails Cloud platform are expected to:

- Use the platform for lawful purposes only, in compliance with all applicable laws and regulations in Zimbabwe and in the jurisdiction from which the platform is accessed
- Respect the rights of Rails Cloud, other customers, and third parties, including privacy rights, intellectual property rights, and contractual rights
- Not use the platform in any manner that degrades the performance, availability, or security of the platform or the experience of other customers
- Maintain accurate and current account registration information
- Take responsibility for all activity conducted under their account credentials
- Report suspected misuse, security vulnerabilities, or AUP violations to aup@railscloud.co

3. Prohibited Uses

The following uses of the Rails Cloud platform are strictly prohibited. Violations are categorised by immediate consequence:

Category	Prohibited Activity	Consequence
Illegal Content	Storing, transmitting, or processing content that is illegal under applicable law, including content that infringes copyright, trademarks, or other IP rights without authorisation	**Immediate suspension**
Child Safety	Any content that exploits, sexualises, or endangers minors in any form	**Immediate termination + law enforcement referral**
Malware	Hosting, distributing, or operating malware, ransomware, spyware, trojans, botnets, or any malicious code	**Immediate termination**
Cyberattacks	Conducting, facilitating, or hosting denial-of-service (DDoS) attacks, port scanning, network intrusion, or any unauthorised access to systems	**Immediate termination + law enforcement referral**
Phishing	Operating phishing sites, credential harvesting pages, or any infrastructure designed to deceive users into revealing sensitive information	**Immediate termination**
Spam	Sending unsolicited bulk email (spam), SMS spam, or operating open mail relays or proxies used for spam distribution	**Immediate suspension**
Cryptocurrency Mining	Mining cryptocurrency using Rails Cloud infrastructure without prior written approval from Rails Cloud	**Immediate suspension**
Sanctions Violations	Using Rails Cloud services in violation of applicable international sanctions, export controls, or trade restrictions	**Immediate termination + regulatory referral**
Platform Abuse	Attempting to circumvent resource limits, billing systems, or access controls; creating multiple accounts to avoid suspension; using automated tools to scrape or stress-test the platform without authorisation	**Suspension + account review**
Unauthorised Resale	Reselling, sublicensing, or providing access to Rails Cloud services to third parties without prior written consent from Rails Cloud	**Suspension + invoice for unauthorised usage**
Interference	Taking any action that materially disrupts or degrades the platform experience for other customers, including excessive resource consumption without a valid enterprise plan	**Suspension + remediation required**

Category	Prohibited Activity	Consequence
Deceptive Practices	Using the platform to impersonate another person or organisation, or to operate fraudulent businesses or investment schemes	Immediate termination + law enforcement referral

4. Content Standards

4.1 Customer Responsibility for Content

Rails Cloud operates as a platform provider and does not monitor or pre-screen Customer Data. Customers are solely responsible for all content stored, transmitted, or processed through their Rails Cloud account. Rails Cloud does not endorse, and is not responsible for, any Customer content.

4.2 Restricted Content Categories

In addition to the absolute prohibitions in Section 3, the following content categories require prior written approval from Rails Cloud before being hosted on the platform:

- Adult content platforms (legal, age-verified, compliant with applicable law)
- Online gambling and gaming platforms subject to licensing requirements
- Pharmaceutical and healthcare marketplaces handling prescription products
- Financial services platforms handling regulated financial instruments or offering financial advice
- Peer-to-peer lending or crowdfunding platforms
- Firearms, ammunition, or controlled substances marketplaces (where legally operated)

To request approval for a restricted content category, contact compliance@railscloud.co with details of your business model, applicable licences, and regulatory compliance framework.

4.3 High-Risk Workloads

Customers operating workloads that process sensitive personal data including health records, financial account data, or government-issued identification data must notify Rails Cloud at enterprise@railscloud.co and ensure appropriate security controls and compliance frameworks are in place.

5. Customer Security Obligations

Customers are responsible for maintaining the security of their own workloads and applications deployed on Rails Cloud infrastructure. Specifically, Customers must:

Obligation Area	Required Actions
Access credentials	Maintain secure passwords and API keys; rotate credentials regularly; revoke access for departed users promptly; never share credentials across accounts

Obligation Area	Required Actions
Application security	Keep all deployed software and dependencies patched and updated; conduct vulnerability assessments on customer-facing applications; remediate known critical vulnerabilities within 72 hours of identification
Network exposure	Limit public network exposure to necessary services only; configure firewalls and security groups appropriately; do not expose administrative interfaces (SSH, RDP, database ports) to the public internet without IP restrictions or VPN
Incident reporting	Report any confirmed or suspected security breach affecting Rails Cloud infrastructure to security@railscloud.co within 24 hours of discovery
Penetration testing	Notify Rails Cloud at least 5 business days before conducting any penetration tests or security assessments of your Rails Cloud environment; do not conduct tests that target Rails Cloud's shared infrastructure

6. Network and Resource Use

6.1 Fair Use

Rails Cloud provides resources based on the subscription tier selected. Customers must use resources within the limits of their plan. Rails Cloud reserves the right to throttle, limit, or suspend resources where usage materially exceeds plan limits or adversely impacts other customers.

6.2 Prohibited Network Activities

The following network activities are prohibited on all Rails Cloud plans:

- Operating open proxies, open relays, or anonymisation services that obscure the origin of traffic for malicious purposes
- Generating or facilitating spoofed, forged, or falsified network traffic
- Conducting network reconnaissance or scanning of IP ranges outside your own allocated infrastructure
- Intentionally consuming bandwidth in excess of plan limits to disrupt service to other customers
- Operating peer-to-peer (P2P) file sharing networks or torrenting infrastructure without prior approval

6.3 Resource Limits and Overages

Customers who consistently and materially exceed their plan resource limits will be contacted by Rails Cloud and required to upgrade to an appropriate plan or implement usage optimisations. Repeated violations after notice may result in service suspension.

7. Rails Pay Specific Acceptable Use

The following additional rules apply specifically to use of the Rails Pay payment platform, in addition to all other AUP provisions:

7.1 Prohibited Transaction Categories

Rails Pay may not be used to process payments for:

- Illegal goods or services under Zimbabwean law or the law of the transaction counterparty's jurisdiction
- Unlicensed money transfer or foreign exchange operations
- Ponzi schemes, pyramid schemes, or fraudulent investment products
- Sanctioned entities, individuals, or jurisdictions under applicable OFAC, UN, or local sanctions lists
- Transactions designed to circumvent currency controls, tax obligations, or financial reporting requirements
- Gambling or gaming operations without applicable regulatory approval and notification to Rails Cloud

7.2 KYC and AML Compliance

All Rails Pay merchants and business accounts must complete Rails Cloud's Know Your Customer (KYC) verification process before processing live transactions. Customers using Rails Pay to process payments on behalf of third parties must implement their own KYC and Anti-Money Laundering (AML) compliance programmes and are responsible for compliance with the Financial Intelligence Unit (FIU) reporting requirements under Zimbabwean law.

7.3 Chargebacks and Disputes

Customers must maintain reasonable chargeback rates. Accounts with chargeback rates exceeding 1% of monthly transaction volume will be placed under review. Accounts exceeding 2% may be suspended from Rails Pay pending remediation. Customers must cooperate fully with Rails Cloud in investigating and resolving payment disputes.

8. Developer API Acceptable Use

Developers accessing Rails Cloud services through the Developer API must comply with the following additional requirements:

- APIs must be accessed using valid, authorised credentials only — credential sharing or pooling is prohibited
- Automated requests must respect published rate limits; deliberate circumvention of rate limiting is a violation of this AUP
- API access must not be used to harvest data from other customers' workloads or from Rails Cloud's internal systems
- Applications built on the Rails Cloud API must themselves comply with this AUP and must not facilitate AUP violations by end users
- Developers must promptly rotate any API keys that are compromised or inadvertently exposed
- Production API keys must not be hardcoded in publicly accessible repositories or client-side code

9. Enforcement

9.1 Investigation

Rails Cloud investigates all reported or detected AUP violations. We may monitor network traffic, review logs, and examine account activity to the extent necessary to investigate suspected violations. We do not routinely monitor Customer content but reserve the right to do so where there is reasonable suspicion of a material AUP violation.

9.2 Enforcement Actions

Depending on the severity and nature of the violation, Rails Cloud may take the following enforcement actions:

Severity	Examples	Action
Minor	First-time resource overuse, minor configuration issues	Written warning
Moderate	Repeated minor violations, spam, unauthorised resale	Temporary suspension + remediation required
Serious	Malware hosting, phishing, cryptocurrency mining	Immediate suspension + formal notice
Critical	Cyberattacks, child safety violations, sanctions breaches	Immediate termination + law enforcement referral

9.3 Notice and Right to Respond

Except where immediate action is required to protect the platform, other customers, or third parties from harm, Rails Cloud will:

1. Notify the Customer of the suspected violation with reasonable detail
2. Provide the Customer with a reasonable opportunity to respond, typically 48 hours for serious violations and 14 days for minor violations
3. Consider the Customer's response before taking enforcement action
4. Provide written confirmation of any enforcement action taken and the basis for it

9.4 Appeals

Customers who believe an enforcement action was taken in error may appeal in writing to aup@railscloud.co within 14 days of the enforcement notice. Appeals will be reviewed by a senior member of the Rails Cloud team not involved in the original enforcement decision. A written determination will be issued within 10 business days of the appeal.

10. Reporting AUP Violations

Rails Cloud encourages responsible reporting of suspected AUP violations on the platform. To report a violation:

- Email aup@railscloud.co with a description of the suspected violation and any supporting evidence
- For urgent security threats (active DDoS, malware distribution, active cyberattack), contact security@railscloud.co — monitored 24/7
- For child safety concerns, contact aup@railscloud.co marked URGENT — these are treated as the highest priority

Rails Cloud will acknowledge all reports within 1 business day and provide a status update within 5 business days. Reporter identity is kept confidential. Rails Cloud does not tolerate retaliation against good-faith reporters.

11. Responsible Vulnerability Disclosure

Rails Cloud operates a responsible disclosure programme for security researchers who identify vulnerabilities in the Rails Cloud platform. If you discover a security vulnerability:

5. Do not exploit the vulnerability or access data beyond what is necessary to confirm its existence
6. Do not publicly disclose the vulnerability before Rails Cloud has had a reasonable opportunity to address it
7. Report the vulnerability to security@railscloud.co with a clear description and steps to reproduce
8. Rails Cloud will acknowledge your report within 48 hours and provide a remediation timeline

Security researchers acting in good faith under this programme will not face legal action from Rails Cloud for their research. Rails Cloud reserves the right to recognise significant discoveries at its discretion.

12. Policy Amendments

Rails Cloud may update this AUP from time to time to reflect changes in law, technology, or platform capabilities. Material changes will be communicated to registered Customers with at least 30 days notice. Continued use of Rails Cloud services following the effective date of an amendment constitutes acceptance.

Where a Customer does not accept a material change to this AUP that directly restricts a use they were previously making, they may terminate the affected Services without penalty within 30 days of the notice.

13. Contact

Query Type	Contact	Response Time
AUP violation reports	aup@railscloud.co	1 business day
Urgent security threats	security@railscloud.co	4 hours (24/7)
Enforcement appeals	aup@railscloud.co	10 business days
Restricted category approvals	compliance@railscloud.co	3 business days

Query Type	Contact	Response Time
Vulnerability disclosure	security@railscloud.co	48 hours
Rails Pay compliance queries	compliance@railscloud.co	2 business days

This Acceptable Use Policy forms part of the Rails Cloud legal framework alongside the Terms of Service, Service Level Agreement, Privacy Policy, Data Processing Agreement, and Data Portability & Exit Policy. All documents available at railscloud.co/legal. Rails Net (Private) Limited, Reg. 84172A0722026, TIN 2002425765, Zimbabwe.