09 553 6489 · info@cloudtria.com · dev.cloudtria.com
PO Box 302379, North Harbour, Auckland 0751, New Zealand

LEGAL & POLICIES

Version 1.3 | Effective 20 November 2026

1. Introduction

This Acceptable Use Policy ("AUP") establishes the rules and conditions governing the use of services, infrastructure, systems and platforms provided by Cloudtria Limited ("Cloudtria", "we", "us" or "our").

Our objective is to maintain a secure, reliable and responsible hosting and technology environment for all customers, partners and users.

This policy applies to all individuals and organisations accessing or using Cloudtria services, whether directly or indirectly, including their employees, contractors, authorised users and end users.

By purchasing, accessing or using any Cloudtria service, you agree to comply with this policy.

2. Scope

This policy applies to all Cloudtria-operated and Cloudtria-provided services, including but not limited to:

- Cloudtria Hosting and associated web hosting services.
- Virtual private servers (VPS), cloud infrastructure and computing resources.
- Domain, DNS and email-related services.
- Cybersecurity services and security platforms.
- Network, connectivity and infrastructure services.
- Customer portals, account management systems and APIs.
- Websites, applications and other services hosted on Cloudtria infrastructure.
- Any other products or services supplied by Cloudtria.

This policy also applies to services accessed through third-party infrastructure providers, where those services are managed, resold or provided by Cloudtria.

09 553 6489 · info@cloudtria.com · dev.cloudtria.com
PO Box 302379, North Harbour, Auckland 0751, New Zealand

3. General responsibilities

You are responsible for ensuring that your use of Cloudtria services complies with this policy and all applicable laws and regulations.

You must:

- Use Cloudtria services lawfully and responsibly.
- Ensure that your activities do not compromise the security, availability or integrity of Cloudtria infrastructure or other customers' services.
- Maintain appropriate security controls over your accounts, applications, systems and hosted content.
- Protect your account credentials, API keys, access tokens and other authentication information.
- Ensure that all individuals using your services comply with this policy.
- Take reasonable steps to prevent your services from being used for malicious or unlawful purposes.
- Respond promptly to security incidents, abuse notifications and requests from Cloudtria.

You remain responsible for activity conducted through your account, including activity performed by authorised users, contractors, applications or compromised systems.

4. Prohibited activities

The following activities are prohibited when using Cloudtria services.

4.1 Illegal activities

You must not use Cloudtria services to facilitate, promote, distribute or engage in activities that violate applicable laws or regulations.

This includes, but is not limited to:

- Fraud, identity theft, financial crime or scams.
- Distribution of stolen, unlawfully obtained or restricted information.
- Distribution of illegal content or materials.

- Copyright, trademark or intellectual property infringement.
- Unlawful surveillance, interception or disclosure of communications.
- Activities that facilitate criminal activity or the exploitation of others.

4.2 Cybersecurity abuse and malicious activity

You must not use Cloudtria services to conduct, facilitate or distribute malicious cyber activity.

Prohibited activities include:

- Deploying, distributing or operating malware, ransomware, spyware, trojans or other malicious software.
- Hosting command-and-control infrastructure for malicious purposes.
- Conducting phishing, credential harvesting or impersonation campaigns.
- Operating botnets or participating in distributed denial-of-service attacks.
- Conducting unauthorised vulnerability scanning, exploitation or penetration testing.
- Attempting to gain unauthorised access to systems, networks, accounts or data.
- Exploiting vulnerabilities in Cloudtria infrastructure or other customers' environments.
- Distributing tools or services specifically intended to facilitate unlawful access or malicious cyber activity.

Security research, vulnerability assessments and penetration testing must only be conducted against systems for which you have explicit authorisation.

You must not conduct security testing against Cloudtria's infrastructure, management systems or other customers' environments without prior written approval from Cloudtria.

4.3 Network abuse and infrastructure misuse

You must not use Cloudtria networks or infrastructure in a manner that negatively impacts other customers, providers or the availability of services.

Prohibited activities include:

- Network flooding, packet amplification or traffic reflection attacks.
- Operating unauthorised open proxies, open relays or publicly accessible anonymisation services where they facilitate abuse.
- Sending spoofed or manipulated network traffic for malicious purposes.
- Deliberately circumventing network restrictions or security controls.
- Interfering with routing, DNS resolution or network availability.
- Conducting activities that create excessive or sustained network congestion.
- Using Cloudtria infrastructure to attack or disrupt third-party networks.

4.4 Email and messaging abuse

Cloudtria services must not be used for unsolicited, deceptive or abusive electronic communications.

Prohibited activities include:

- Sending unsolicited bulk email (spam).
- Operating unauthorised bulk mailing or spam distribution systems.
- Sending phishing, fraudulent or deceptive messages.
- Distributing malware or malicious links through email.
- Operating open SMTP relays or compromised mail servers.
- Forging email headers or sender identities to conceal the origin of messages.
- Using purchased, harvested or otherwise unlawfully obtained mailing lists.
- Continuing to send communications to recipients who have withdrawn consent or opted out, where applicable.

Customers operating legitimate email services must maintain appropriate sender authentication and security controls, including SPF, DKIM and DMARC where supported and applicable.

09 553 6489 · info@cloudtria.com · dev.cloudtria.com
PO Box 302379, North Harbour, Auckland 0751, New Zealand

4.5 Content and hosting restrictions

You must not host, publish, distribute or facilitate access to content that is unlawful or otherwise prohibited under this policy.

This includes:

- Child sexual abuse material or content involving the exploitation of minors.
- Content promoting terrorism or violent extremist activity.
- Content used to facilitate fraud, scams or financial deception.
- Unauthorised distribution of copyrighted or protected material.
- Content that unlawfully exposes private, confidential or personal information.
- Content that facilitates harassment, threats, abuse or exploitation.

Cloudtria reserves the right to investigate reports of prohibited content and take appropriate action where necessary.

4.6 Resource abuse and excessive usage

You must use allocated hosting, storage, processing, memory and network resources in accordance with your service plan and any applicable fair-use or resource limits.

Prohibited activities include:

- Deliberately consuming excessive resources in a manner that degrades services for other customers.
- Circumventing service limits, quotas or technical restrictions.
- Running uncontrolled processes that negatively impact shared infrastructure.
- Using services for unauthorised cryptocurrency mining or other resource-intensive activities that exceed permitted service usage.
- Operating persistent workloads that are incompatible with the purchased service or its intended purpose.

Cloudtria may apply resource restrictions, request workload adjustments or recommend an alternative service where

09 553 6489 · info@cloudtria.com · dev.cloudtria.com
PO Box 302379, North Harbour, Auckland 0751, New Zealand

usage is inconsistent with the purchased service.

5. Security and account responsibilities

Customers are responsible for maintaining the security of their accounts, hosted applications and systems.

You must:

- Use strong and unique passwords.
- Enable multi-factor authentication where available.
- Keep operating systems, applications and software appropriately patched.
- Remove unnecessary services, accounts and access permissions.
- Secure databases, administrative interfaces and remote access services.
- Monitor your systems for suspicious activity.
- Maintain appropriate endpoint and application security controls.
- Notify Cloudtria promptly if you suspect an account compromise or security incident.

You must not knowingly allow compromised, vulnerable or misconfigured systems to remain operational where they present a material risk to Cloudtria infrastructure or other customers.

Cloudtria may require remedial action where a customer's systems present a security risk.

6. Customer data and hosted content

You retain responsibility for the data, applications, websites and other content that you store, process, transmit or make available using Cloudtria services.

You are responsible for:

- Ensuring you have the necessary rights and permissions to use and distribute your content.
- Ensuring your collection and processing of personal information complies with applicable privacy requirements.
- Implementing appropriate data protection and access controls.

- Maintaining backups appropriate to your business and operational requirements.
- Ensuring your hosted applications do not expose or compromise information belonging to other parties.

Cloudtria does not assume responsibility for the legality or accuracy of customer-provided content.

7. Vulnerability disclosure and security research

Cloudtria recognises the importance of responsible security research and vulnerability disclosure.

If you identify a potential vulnerability affecting Cloudtria services or infrastructure, you should report it to Cloudtria through an appropriate support or security contact channel.

You must not exploit, disclose or publicly demonstrate a vulnerability in a manner that could compromise systems, expose customer information or disrupt services.

All security testing involving Cloudtria-owned or managed infrastructure requires prior written authorisation.

Nothing in this section grants permission to access systems or data that you do not own or have explicit authorisation to test.

8. Monitoring and investigation

Cloudtria may monitor service usage, network activity and security events to the extent reasonably necessary for:

- Maintaining the security and availability of services.
- Detecting and investigating malicious or abusive activity.
- Enforcing this policy and applicable service agreements.
- Responding to security incidents and abuse reports.
- Complying with applicable legal obligations.

Cloudtria may investigate suspected violations of this policy and may request information or cooperation from affected customers.

Monitoring and investigations will be conducted subject to applicable privacy and legal requirements.

09 553 6489 · info@cloudtria.com · dev.cloudtria.com
PO Box 302379, North Harbour, Auckland 0751, New Zealand

9. Reporting abuse and security incidents

Customers and third parties are encouraged to report suspected misuse, security incidents, malicious activity or violations of this policy to Cloudtria.

Reports should include, where available:

- The affected domain, IP address or service.
- A description of the suspected activity.
- Relevant timestamps and time zones.
- Supporting evidence, logs or URLs.
- Any relevant incident or reference information.

Reports should be submitted through Cloudtria's available support channels at:

https://www.cloudtria.com

Customers must notify Cloudtria promptly if they become aware that their account, hosted systems or services have been compromised or are being used for malicious activity.

10. Enforcement and corrective action

Cloudtria reserves the right to take appropriate action when a violation of this policy is identified or reasonably suspected.

Depending on the nature, severity and circumstances of the incident, actions may include:

- Issuing a warning or requesting corrective action.
- Requiring the removal of prohibited content or applications.
- Restricting network access or specific service functionality.
- Suspending affected services or accounts.
- Blocking malicious traffic or abusive network activity.

09 553 6489 · info@cloudtria.com · dev.cloudtria.com
PO Box 302379, North Harbour, Auckland 0751, New Zealand

- Temporarily isolating compromised systems.
- Disabling affected credentials or access tokens.
- Terminating services where a serious or repeated breach occurs.
- Reporting suspected unlawful activity to relevant authorities where appropriate or legally required.

Cloudtria may take immediate action without prior notice where necessary to protect its infrastructure, customers, third parties or the wider internet from an imminent or material security threat.

Where reasonably practicable, Cloudtria will notify affected customers of enforcement actions and provide information about the steps required to address the issue.

11. Reinstatement of services

Where a service has been restricted or suspended due to a breach of this policy, Cloudtria may require the customer to demonstrate that the underlying issue has been resolved before restoring access.

Reinstatement may be subject to:

- Removal of malicious or prohibited content.
- Remediation of compromised systems.
- Implementation of appropriate security controls.
- Confirmation that the activity will not recur.
- Payment of any applicable outstanding charges.

Cloudtria reserves the right to refuse reinstatement where the risk remains unacceptable or where the customer has repeatedly breached this policy.

12. Third-party services and providers

Cloudtria may rely on third-party infrastructure providers, network operators, software vendors and service partners to deliver its services.

Customers must also comply with any applicable acceptable use requirements imposed by those providers.

Where a third-party provider identifies prohibited activity or requires Cloudtria to take action, Cloudtria may implement appropriate restrictions or enforcement measures to maintain compliance with those requirements.

13. Consequences of policy violations

Violations of this policy may constitute a breach of the applicable service agreement, Terms of Service or other contractual obligations between you and Cloudtria.

Cloudtria reserves all rights and remedies available under the applicable agreements and relevant law.

You may be responsible for costs, losses or damages arising from your breach of this policy to the extent provided under the applicable service agreement and law.

14. Changes to this policy

Cloudtria may update this Acceptable Use Policy from time to time to reflect changes in technology, services, security requirements, operational practices or applicable legal obligations.

Updated versions will be published on the Cloudtria website with a revised effective date.

Continued use of Cloudtria services following the effective date of an updated policy constitutes acceptance of the updated policy, to the extent permitted by applicable law and the relevant service agreement.

15. Contact information

For questions about this policy, suspected abuse or security incidents, please contact Cloudtria through the support channels available on our website.

Cloudtria Limited

Website: https://www.cloudtria.com
Support: https://www.cloudtria.com

© 2026 Cloudtria Limited. All Rights Reserved.