Zeniar
Perth, Western Australia, Australia
ABN 57295582608

Acceptable Usage Policy (AUP)

This Acceptable Use Policy ("Policy") outlines acceptable and unacceptable use of services provided by Zeniar ("we", "us", or "our"). This Policy is designed to protect our network, customers, and the internet community from inappropriate, illegal, or otherwise harmful activities. By using our services, you agree to be bound by this Policy, in addition to our Terms of Service.

Illegal or Harmful Use

You may not use Zeniar services to engage in, promote, or facilitate illegal, abusive, or harmful activities. This includes, but is not limited to:

- Accessing, storing, or distributing illegal content such as child exploitation material, pirated software, or stolen data.
- Hosting or distributing content that violates copyright, trademark, or other intellectual property rights.
- Using our services to engage in fraud, phishing, identity theft, or other deceptive practices.
- Hosting phishing pages, credential-harvesting sites, or web pages designed to deceive users into disclosing personal or financial information.
- Hosting or distributing malware, ransomware, spyware, trojans, viruses, or any other malicious software.
- Operating command-and-control (C2) infrastructure for botnets, malware, or any other malicious network activity.

We comply with all applicable Australian laws, including the Criminal Code Act 1995 (Cth) and Telecommunications Act 1997 (Cth).

Security Violations

Our services must not be used to compromise the security, integrity, or availability of any system. This includes:

- Deploying or participating in denial-of-service (DoS or DDoS) attacks.
- Operating or being part of a botnet.
- Attempting to gain unauthorised access to any system, service, or network.
- Operating IRC servers or similar relay chat infrastructure commonly used in botnet coordination.
- Conducting port scanning, network probing, or vulnerability scanning of third-party systems without authorisation.

Spam and Unsolicited Messaging

Zeniar has zero tolerance for spam. You may not use our services to:

- Send bulk unsolicited messages, including emails and instant messages.
- Operate mailing lists without explicit opt-in consent from recipients.
- Promote websites or services through deceptive or unsolicited channels.

All email use must comply with the Spam Act 2003 (Cth).

Resource Abuse

Zeniar hosting plans are not intended to function as general-purpose cloud storage or file backup services. You must not:

- Use your hosting account for personal file storage, backups, or archiving unrelated to your hosted website or application.
- Host large files exceeding 1 GB in size without our prior written consent.
- Consume server resources in a way that impacts the performance or availability of other users' services.
- Mine cryptocurrency or perform any computationally intensive financial or blockchain-related workloads on Zeniar's infrastructure. This prohibition applies regardless of the type of currency, consensus mechanism, or scale of the operation.
- Host or operate peer-to-peer (P2P) file-sharing applications, BitTorrent trackers, seedboxes, or similar services that generate disproportionate bandwidth consumption or facilitate copyright infringement.
- Operate open proxies, anonymisation services, VPN endpoints, or relay services that could be used to mask the origin of traffic or circumvent access controls.

Prohibited Hosted Services and Applications

The following types of services, platforms and applications may not be hosted on Zeniar's infrastructure:

Large Language Models (LLMs) and AI Inference Services: You may not host, operate, or make available any large language model, AI inference endpoint, machine learning model serving infrastructure, or similar computationally intensive AI workload on Zeniar's shared hosting infrastructure. This includes, but is not limited to, self-hosted LLM instances (e.g. Llama, Mistral, GPT variants), AI API proxies, or automated AI-generated content pipelines that impose significant CPU, RAM or storage load beyond normal website usage.

Deepfake Platforms and Content: You may not host any website, service, application or content repository whose primary or significant purpose is the creation, storage, distribution, or promotion of deepfake content. This includes platforms or tools designed to synthetically alter the likeness, voice, or actions of real individuals without their consent, regardless of whether the content is presented as entertainment, satire, or otherwise. See also the *False, Misleading or Extremist Content* section regarding the distribution of deepfake content for deceptive or defamatory purposes.

Adult Content

Zeniar permits the hosting of legal adult content on paid hosting plans subject to all of the following conditions:

- The content must be hosted under a domain name where the applicable top-level domain (TLD) permits adult content. Adult content is strictly prohibited on Zeniar's free subdomains under the .zhost.au domain in accordance with auDA domain policies governing the .au namespace.
- All adult content must be legal under applicable Australian law, including but not limited to the Classification (Publications, Films and Computer Games) Act 1995 (Cth), the Online Safety Act 2021 (Cth), and any relevant state or territory legislation.
- Content that sexually depicts, exploits, or targets minors is absolutely prohibited and will be reported to the Australian Federal Police and the Australian Centre to Counter Child Exploitation (ACCCE).
- You are solely responsible for implementing all applicable age verification requirements, content classification obligations, and any other compliance obligations under Australian law.
- Zeniar reserves the right to remove any adult content that it determines, in its sole discretion, to be unlawful, in breach of this Policy, or otherwise harmful, without prior notice.

False, Misleading or Extremist Content

You may not use our services to publish, promote, or distribute:

- Extremist political or religious views that promote violence, discrimination, or hate.
- Content intended to mislead others, including disinformation or narratives designed to manipulate public opinion through false or fabricated information.
- Deepfake content or AI-generated media used to impersonate individuals or spread false impressions, particularly where the intent is to deceive or defame. See also the *Prohibited Hosted Services and Applications* section regarding the hosting of deepfake platforms.
- Edited video or audio clips that misrepresent political figures, groups, or individuals in a misleading or malicious way.

Zeniar reserves the right to remove content that violates this section and to suspend associated services at our sole discretion.

Enforcement

Zeniar will respond to policy breaches in a proportionate and escalating manner. The following framework outlines the standard process, though Zeniar reserves the right to take immediate action at any stage where the severity of the breach warrants it:

Stage 1 — Warning (First breach, no impact on other customers)

Zeniar will send a written notification to the Subscriber's registered email address identifying the breach and the required remediation. The Subscriber must acknowledge the notification and advise Zeniar of the steps taken to remedy the breach. Failure to respond or remedy the breach may result in immediate suspension without further warning.

Stage 2 — Immediate Suspension (Breach causing impact to other customers)

Where a breach is causing degradation of service or harm to other customers, Zeniar will immediately suspend the offending Service(s) without prior notice. A written notification will then be sent to the Subscriber requesting acknowledgement and remediation. Services will only be reactivated once the Subscriber has acknowledged the breach and Zeniar is satisfied the issue has been resolved. No reactivation fee applies.

Stage 3 — Suspension with Prior Breach (Repeat breach within 3 months)

Where a Subscriber commits a breach and has recorded a prior breach within the preceding 3 months, the Service(s) will be immediately suspended. Reactivation requires the Subscriber to acknowledge the breach and provide Zeniar with a satisfactory remediation plan. No

reactivation fee applies.

Stage 4 — Termination (Three or more breaches within 3 months)

Where a Subscriber has committed three or more breaches within any 3-month period, Zeniar reserves the right to immediately suspend the Service(s) and issue a written notice requiring the Subscriber to migrate their data and services to an alternative provider. If the Subscriber does not respond within 7 days, the Service(s) will be terminated without further notice.

Following termination under this stage, the Subscriber may request a backup of their data within 30 days of the termination date for a fee of $149.00 AUD. Zeniar does not guarantee that data will be available or restorable, and payment of the fee does not guarantee a successful recovery. After 30 days, all data may be permanently and irrecoverably deleted.

Immediate Termination (Serious Violations)

Notwithstanding the above, Zeniar reserves the right to immediately terminate any Service(s) without notice and without progressing through the stages above where the breach involves: child exploitation material; malware or botnet hosting; denial-of-service attacks; or any other activity that is illegal or poses an immediate and seriousrisk to Zeniar's infrastructure, other customers, or the public. Zeniar will cooperate fully with law enforcement authorities in such cases.

The Subscriber will be solely liable for any costs or fees paid by Zeniar to third-party providers to remediate restrictions or blocks imposed as a result of the Subscriber's breach of this Policy.

Responsibility and Compliance

You are responsible for the content you host and the activity that occurs under your account. You must ensure compliance with this Policy, as well as all applicable Australian laws, including the Copyright Act 1968 (Cth), Online Safety Act 2021 (Cth), and any other relevant legislation.

Changes to This Policy

We may update this Policy at any time. All changes will be posted to our website. Continued use of Zeniar services after changes are published constitutes acceptance of the revised Policy.

END OF DOCUMENT