

Acceptable Use Policy

Last Updated: July 10, 2026

1. Introduction & Scope

This Acceptable Use Policy ("AUP") explains what is and is not permitted on any service provided by Ceohost ("Ceohost," "we," "us," "our"), including Shared Hosting, WordPress Hosting, India Hosting, Reseller Hosting, VPS, Cloud Hosting, and Dedicated Servers. This AUP applies to every customer, every account, and every website, application, or service hosted with us, and should be read together with our Terms of Service.

Our aim is to keep this policy explicit and predictable, not a vague "we can suspend you for anything" clause. Violations may result in a warning, suspension, or immediate termination depending on severity, as described in Section 27 (Enforcement).

To report abuse on any Ceohost-hosted website or service, please email abuse@ceohost.in with the URL, a timestamp, and supporting evidence.

2. Definitions

- **"Customer"** means the individual or entity that has purchased or registered for a Ceohost service.
- **"Account"** means the hosting account, VPS, server, or associated resources provisioned for a Customer.
- **"Service"** means any hosting, domain, email, VPS, Cloud, Dedicated Server, or related offering provided by Ceohost.
- **"Content"** means any data, files, code, text, image, video, or other material uploaded, stored, or transmitted using the Service.
- **"Abuse"** means any activity that violates this AUP, our Terms of Service, or applicable law, or that degrades the security, stability, or performance of Ceohost's network or other customers' services.

3. Prohibited Content

The following categories of content may not be uploaded, stored, hosted, transmitted, or linked to from any Ceohost service:

- **Child Sexual Abuse Material (CSAM)** or any content that sexualizes or endangers minors — treated with zero tolerance, resulting in immediate account termination and mandatory reporting to the National Crime Records Bureau / CBI Cyber Crime Cell and, where applicable, international bodies such as NCMEC.
- Content promoting terrorism, real-world violence, or that provides instructions/encouragement for self-harm or violent acts.
- Non-consensual intimate imagery ("revenge porn") or any content that sexualizes or exposes a person without their consent.

- Content that infringes on third-party intellectual property, including pirated software, unlicensed media, or trademark-infringing material (see Section 31, Content Complaints, and Section 14, Repeat Copyright Infringer Policy).
- Malware, ransomware, phishing pages, botnet command-and-control (C2) infrastructure, or exploit kits of any kind.
- Content facilitating illegal drugs, weapons, explosives, or human trafficking.
- Content that promotes or facilitates illegal gambling, betting, or lottery schemes not licensed under applicable Indian law.
- Hate speech, or content that incites violence or discrimination against any individual or group based on religion, caste, race, gender, sexual orientation, or nationality.
- Defamatory content directed at any individual, organization, or community.
- Content that violates a person's privacy or right of publicity, including publishing someone's private information without consent.
- Cryptocurrency mining scripts or software, unless you have obtained Ceohost's express written approval in advance (typically only available on eligible VPS/Dedicated plans).

4. Prohibited Activities

The following activities are not permitted on any Ceohost service:

- **Network Abuse:** Port-scanning, IP-scanning, or brute-forcing login credentials against any third-party service, website, or server.
- **Open Relays/Proxies/Resolvers:** Running open mail relays, open proxies, open DNS resolvers, or anonymizer services that can be exploited by third parties for abuse.
- **File-Sharing Infrastructure:** Hosting torrent trackers, magnet-link indexes, or public file-sharing/warez indexes.
- **IRC Servers:** Running IRC servers or IRC bots on Shared or Reseller Hosting plans (permitted only on VPS/Dedicated, subject to other AUP restrictions).
- **Games Hosting:** Hosting game servers on Shared, WordPress, or Reseller Hosting plans (see our Terms of Service, Section 11 — games are permitted only on VPS/Dedicated plans).
- **Unauthorized Reselling:** Reselling hosting resources on non-Reseller plans, as detailed in our Terms of Service, Section 4.
- **Credential/Account Abuse:** Sharing, selling, or using another customer's hosting account or credentials without authorization.
- **Impersonation:** Impersonating any other individual, business, or organization, or falsely claiming affiliation with a person or entity you do not represent.
- **Harassment:** Using any Ceohost service to threaten, stalk, harass, or send unwanted repeated communications to any individual.
- **Unauthorized Data Collection:** Scraping, harvesting, or collecting personal information (such as email addresses or phone numbers) about other individuals without their consent, for spamming, resale, or any other unauthorized purpose.

5. Email Reputation & Blacklisting Policy

Because mail servers are shared infrastructure, one account's poor email practices can affect deliverability for every customer on that server. Accordingly:

- Customers must follow good email practices: valid opt-in recipient lists, a working unsubscribe mechanism for any bulk/marketing email, and accurate sender information.
- If an account's sending activity causes the shared mail server's IP address to be listed on a recognized email blacklist (e.g., Spamhaus, SORBS), Ceohost may immediately suspend that account's email sending capability to protect deliverability for all other customers, pending investigation.
- Repeated blacklisting incidents traced to the same account may result in permanent suspension of mail services for that account, or a requirement to move to an isolated/dedicated IP solution at the customer's cost.

6. SMTP / Email Sending Limits

- Current sending limits are published in our Terms of Service and/or Knowledge Base and may be changed by Ceohost from time to time to reflect infrastructure and deliverability needs.
- Customers requiring higher-volume transactional or marketing email sending should use a dedicated third-party email delivery service (e.g., an authenticated transactional email API) rather than routing bulk volumes through standard hosting mailboxes.
- Ceohost may throttle or temporarily disable SMTP access on an account showing sending patterns consistent with spam or compromised-account abuse, pending customer verification.

7. VPN, Proxy & Tor Exit Node Policy

Running a public VPN service, open proxy service, or a Tor exit node on Shared, WordPress, or Reseller Hosting plans is not permitted, as these commonly attract network abuse that can affect the shared server's IP reputation. Such use cases may be considered on a VPS or Dedicated Server plan only with prior written approval from Ceohost, subject to additional terms.

8. SEO Spam Policy (Hidden Text, Cloaking, Doorway Pages)

Manipulative SEO techniques that violate search engine guidelines and can be used to deceive users are not permitted, including:

- Hidden or invisible text/links designed solely to manipulate search rankings;
- Cloaking (showing different content to search engines than to human visitors);
- Doorway pages or auto-generated low-quality pages created solely to rank for search queries and redirect users elsewhere;
- Large-scale automated content-spinning or link-farm networks hosted primarily for search manipulation purposes.

9. Fake Reviews, Fake Followers & Fake Traffic Policy

Using Ceohost services to generate, host, or operate tools/scripts for fake reviews, fake social media followers/engagement, or artificially inflated website traffic/click-fraud is prohibited, as such activity is generally deceptive to consumers and may violate consumer-protection or platform-specific laws.

10. High-Risk Financial Services Policy

Ceohost does not permit hosting of websites or applications engaged in unlicensed or fraudulent financial activity, including but not limited to Ponzi/pyramid schemes, fake loan or fake investment platforms, unregistered forex/trading signal scams, or any scheme designed to defraud users of money. Legitimate financial services are welcome, provided they are properly licensed under applicable law in the jurisdiction(s) they operate in, subject to providing relevant licensing documentation on request.

11. Bot & API Abuse Policy

Automated bots, scripts, or API integrations hosted on Ceohost services must not be used to overload third-party services, bypass rate-limits/CAPTCHAs on other platforms, conduct credential-stuffing attacks, or perform any activity that would reasonably be considered abusive automation against a third party. Ceohost also reserves the right to rate-limit or restrict any bot/API traffic on our own infrastructure that threatens server stability.

12. Domain Abuse Policy (Typosquatting, Fast-Flux DNS)

Registering or using domain names for typosquatting (deliberately misspelled variations of trademarked/well-known domains) to deceive users, or operating fast-flux DNS infrastructure typically associated with malware/botnet resilience, is strictly prohibited and will result in immediate domain/account suspension.

13. Cryptocurrency Scam Policy

Hosting of fraudulent cryptocurrency schemes is strictly prohibited, including fake Initial Coin Offerings (ICOs), fraudulent token launches, wallet-drainer scripts, phishing pages impersonating legitimate crypto exchanges/wallets, or any tool designed to deceive users into transferring cryptocurrency under false pretenses. This is separate from the legitimate crypto-mining approval process described in Section 3.

14. AI Misuse Policy (Deepfakes, AI Phishing, Voice-Clone Fraud)

Use of Ceohost services to create, host, or distribute AI-generated deepfake content intended to deceive or defame a real person, AI-generated phishing content, voice-cloning used for fraud or impersonation (e.g., fake calls impersonating a real person for financial fraud), or any other malicious use of AI/synthetic media to deceive, defraud, or harm an individual or organization is strictly prohibited and will result in immediate suspension and potential referral to law enforcement.

15. Repeat Copyright Infringer Policy

In line with our Content Complaints process (Section 31), Ceohost maintains a repeat-infringer policy: an account that receives **three or more substantiated copyright infringement complaints** within a 12-month period will be considered for permanent termination, regardless of whether each individual complaint was resolved by content removal. Ceohost may take earlier action, including immediate suspension, where the severity or scale of a single infringement reasonably warrants it, without needing to wait for a third complaint.

16. Resource & Network Usage Limits

Fair and reasonable resource usage keeps our servers fast and stable for every customer sharing that infrastructure. The following limits apply in addition to the plan-specific limits described in our Terms of Service:

- **Sustained CPU Usage:** On Shared and Reseller Hosting, sustained CPU usage above 25% for longer than 90 continuous seconds is considered a violation of fair usage (VPS and Dedicated Server plans, where resources are dedicated to the customer, are exempt from this specific limit, subject to their own plan specifications).
- **Bandwidth & Storage:** As detailed in our Terms of Service (Sections 5 and 9), storage and bandwidth are subject to fair-use thresholds even on "Unlimited" plans.
- **Database & Query Limits:** Long-running queries, oversized databases, and high-frequency cron jobs are restricted as detailed in our Terms of Service, Section 4.
- Accounts exceeding these limits will typically receive an optimization notice before any suspension, except where the usage is actively degrading service for other customers, in which case immediate throttling may be applied.

17. Excessive Inodes / Millions of Small Files

Accounts storing an unusually high number of small files (e.g., millions of tiny cache, session, or log files) beyond the inode limits described in our Terms of Service may significantly impact filesystem and backup performance. Such accounts will be asked to clean up or archive unnecessary files, or to move to a VPS/Dedicated solution suited to high file-count workloads.

18. Fork Bomb, Infinite Loop & Resource Exhaustion Policy

Intentionally or negligently running scripts that create fork bombs, infinite loops, memory-exhaustion routines, or any process designed to (or that has the effect of) exhausting shared server resources is strictly prohibited and will result in immediate process termination and, for repeated incidents, account suspension.

19. Background & Long-Running Process Restrictions

Persistent background daemons, long-running scripts, or continuously-executing processes (outside of standard cron jobs within the limits in our Terms of Service) are not permitted on Shared or Reseller Hosting plans, as these plans are designed for standard request-response website workloads. Such use cases require a VPS or Dedicated Server plan.

20. Public Download, File-Mirror & CDN Hosting Restriction

Using Shared or Reseller Hosting as a public file-download mirror, software repository mirror, or a general-purpose CDN/media-delivery node for high-volume third-party traffic is not permitted, as this workload pattern is disproportionate to standard website hosting. Customers with such requirements should use a VPS, Dedicated Server, or discuss a custom solution with our sales team.

21. Temporary File Storage Restriction

Temporary/cache directories should not be used for long-term file storage. Ceohost reserves the right to periodically clear temporary directories that are not part of standard, actively-used application functionality,

without separate notice, as part of routine server maintenance.

22. URL Shortener Abuse Policy

Operating a public URL-shortening service on Ceohost infrastructure that is used to mask phishing links, malware distribution links, or other malicious destinations is strictly prohibited and will result in immediate suspension of the offending service.

23. Dedicated Server – Specific Rules

Customers with root/administrative access on a Dedicated Server are responsible for securing their own operating system, firewall configuration, and installed software. Ceohost is not responsible for the security configuration of a Dedicated Server beyond the physical hardware and network layer, but reserves the right to null-route, isolate, or suspend a Dedicated Server that is actively attacking other systems, distributing malware, or otherwise endangering network stability, regardless of the customer's administrative control over that server.

24. Security Research & Penetration Testing Rules

You may perform security testing or penetration testing only against your own website/application hosted with Ceohost, and only after providing prior written notice to abuse@ceohost.in describing the scope and timing of the test. Security testing against any other customer's account, or against Ceohost's own infrastructure, without express written authorization, is strictly prohibited and will be treated as a serious violation under Section 27.

25. Additional KYC Verification for Suspicious Accounts

In addition to the standard KYC requirements described in our Terms of Service, Ceohost reserves the right to request additional identity verification or documentation at any time from any account showing patterns associated with fraud, abuse, or policy violations (for example, unusual payment patterns, multiple accounts from the same source attempting prohibited activity, or content flagged in an abuse investigation). Failure to provide requested additional verification within a reasonable timeframe may result in suspension of the account pending compliance.

26. Evidence Preservation During Investigations

Where Ceohost is investigating a suspected AUP violation, we may preserve relevant account data, logs, and content for a reasonable period necessary to complete the investigation and to comply with any related legal process, even if the account is otherwise suspended or scheduled for standard data deletion under Section 29 (Suspension for Non-Renewal & Data Retention). This preserved data is handled in accordance with our Privacy Policy and is not used for any purpose beyond the investigation and applicable legal compliance.

27. Enforcement

Ceohost applies a proportionate, predictable enforcement approach based on the severity of the violation:

- **Minor Violations** (e.g., first-time resource-limit breach, minor configuration issues): a notice is sent with a **48-hour cure period** to fix the issue before any suspension.

- **Spam Violations:** a **3-strike policy** applies — a warning on the first two verified complaints, with suspension considered on the third, or immediately for large-scale/malicious spam campaigns.
- **Emergency Suspension Without Notice:** For serious violations posing an active, immediate risk — including but not limited to CSAM, active malware distribution, phishing infrastructure, confirmed large-scale spam, DDoS-source activity, or any activity threatening the security or stability of our network or other customers — Ceohost reserves the right to **immediately suspend the account without prior notice**, followed by customer notification as soon as reasonably possible, and, where legally required, a report to the appropriate authority.
- **Appeals:** If you believe an enforcement action was taken in error, you may submit an appeal via support ticket. We aim to review and respond to all appeals within **48 hours**.
- **Logging:** Enforcement actions are logged internally for accountability and, where relevant to a legal or regulatory process, may be disclosed as required by law.

28. False Abuse Report Policy

Submitting a knowingly false, malicious, or bad-faith abuse report — for example, to harass a legitimate competitor or customer, or to trigger unwarranted suspension of an account — is itself a violation of this AUP. Ceohost reserves the right to disregard reports found to be made in bad faith, and, where a pattern of false reporting is identified from a particular source, to restrict that source's ability to submit further reports and/or take other appropriate action.

29. Suspension for Non-Renewal & Data Retention

If a service is not renewed by its due date, it will be suspended in accordance with our Terms of Service (Section 14, Payment, Billing & Late Payment Policy). In addition to those billing timelines, the following applies specifically to account data during a suspension:

- Once an account is suspended for non-renewal, it enters a **14-day grace/hold period**. During this period, your data is retained but the account is not publicly accessible, and should be considered to be in an **"unsafe/at-risk" data state** — i.e., not guaranteed to be fully protected or recoverable, since it is outside normal active-service handling.
- If payment/renewal is not completed within this 14-day period, Ceohost reserves the right to **permanently delete all associated data**, including website files and databases, without further notice.
- Depending on the circumstances (server capacity, plan type, or account history), Ceohost may, at its discretion, delete data before the full 14 days in certain cases, or extend it in others — the 14-day period is a general guideline, not a guaranteed minimum in every situation.
- We strongly recommend renewing before the due date, or downloading an independent backup of your data promptly, to avoid any risk of data loss during a suspension period.

30. Backup Responsibility – Shared Responsibility

As described in our Terms of Service (Section 7, Backup Policy), Ceohost provides a complimentary backup service as a courtesy. However, backup is a **shared responsibility**:

- Ceohost's backup service is supplementary and not a guaranteed data-protection system — it can fail, be delayed, or be affected by technical issues like any system.

- You, as the customer, remain responsible for independently backing up your own critical website files, databases, and any other important data on a regular basis, using your own local copies, third-party backup tools, or manual downloads.
- This shared responsibility applies at all times, including during normal operation, before making major changes to your website, and especially during any suspension period as described in Section 29.

31. Content Complaints (DMCA / IT Act / Defamation)

If you believe content hosted on a Ceohost customer's website infringes your copyright, violates the Information Technology Act, or is defamatory, please send a complaint to **abuse@ceohost.in** including:

- The specific URL(s) of the content in question;
- Identification of the copyrighted work or a description of the legal basis for your complaint;
- Your contact details and, where applicable, proof of your identity/authority to act on behalf of the rights holder;
- A statement of good-faith belief that the use is unauthorized or unlawful.

We aim to respond to all valid content complaints within **48 hours**. Where a complaint is substantiated, we may remove or disable access to the content and notify the affected customer, who may submit a counter-notice as permitted under applicable law (see also our Terms of Service, Section 22, Copyright Complaints, and Section 15, Repeat Copyright Infringer Policy).

32. Reporting Abuse

Anyone — customer or non-customer — may report suspected abuse on a Ceohost-hosted website or service by emailing **abuse@ceohost.in**. Anonymous reports are welcome and will be investigated (see also Section 28, False Abuse Report Policy). Ceohost does not disclose a reporter's identity to the reported party, except where legally compelled to do so by a court order or law-enforcement request.

- **CSAM or active-malware reports:** Ceohost aims to act within **4 hours** of a verified report.
- **All other abuse reports:** Ceohost aims to act within **48 hours** of a verified report.

33. Law Enforcement & Regulatory Cooperation

Ceohost cooperates with law-enforcement agencies, courts, and regulatory authorities in India in accordance with applicable law, including the Information Technology Act, 2000 and CERT-In directions. Where legally required, Ceohost may disclose account information, content, or logs pursuant to a valid legal request, subpoena, or court order, as further described in our Privacy Policy.

34. Hosting Space Use

Hosting space is for active website content only; files should generally be linked to and accessible from your website (see our Terms of Service, Section 5, regarding the 300GB fair-use threshold).

35. Customer Security Responsibility

You are responsible for keeping your account and application passwords confidential and your CMS/plugins/scripts updated and patched. Ceohost may temporarily suspend a compromised account to protect other customers on shared infrastructure.

36. IP Address Ownership

Any IP address assigned to your account remains the property of Ceohost and is allocated for your use only for the duration of your subscription (see our Terms of Service, Section 15.1).

37. AI-Generated Content Responsibility

If you host AI-generated content, chatbots, or automated agents, you are solely responsible for reviewing that content/output and ensuring it does not violate this AUP or applicable law.

38. Monitoring Rights

Ceohost reserves the right, though is not obligated, to monitor or investigate account activity where abuse or a security threat is reasonably suspected, in line with our Privacy Policy. Routine, proactive monitoring of customer content is not performed; monitoring occurs only in response to a specific report, complaint, or reasonably suspected security/abuse issue.

39. Sole Determination of Violations

Ceohost has the sole right to reasonably determine whether an activity or content item violates this AUP, and to decide the appropriate corrective action, subject to the appeal process in Section 27.

40. No Refund for AUP-Related Suspension or Termination

Where an account is suspended or terminated due to a confirmed AUP violation, no refund is issued for the remaining/unused portion of the affected service, consistent with our Refund Policy, Section 18.

41. Our Commitment on Technical Issues

Ceohost's infrastructure and technical teams work hard to keep our servers stable, secure, and performant. While no hosting provider can guarantee a completely issue-free experience at all times, we treat technical issues as rare exceptions, not the norm, and we invest continuously in monitoring, redundancy, and rapid response to keep disruptions to an absolute minimum for every customer.

42. Severability

If any provision of this Acceptable Use Policy is found to be invalid or unenforceable by a competent authority, that provision shall be limited or eliminated to the minimum extent necessary, and the remaining provisions of this AUP shall continue in full force and effect.

43. Relationship to Other Policies

This AUP works together with, and does not replace, our Terms of Service (which covers KYC, resource limits, fair-usage thresholds, and account-level consequences), our Refund Policy (which explains that accounts suspended/terminated for AUP violations are not eligible for a refund), and our Privacy Policy (which explains how we handle data related to abuse investigations).

44. Changes to This Policy

Ceohost may update this Acceptable Use Policy at any time, at its sole discretion, to address new types of abuse, emerging security threats, or legal/regulatory requirements. The version published on our website at the time of any enforcement action will govern. Continued use of our Services after an update constitutes acceptance of the revised AUP.

45. Contact Us

For abuse reports: **abuse@ceohost.in**. For general AUP questions: **support@ceohost.in** or visit www.ceohost.in/contact.