

Acceptable Use Policy

Updated September 17, 2026 | discountrouter.ai

1. Scope and responsibility

This Acceptable Use Policy ("AUP") applies to all use of DiscountRouter Services and forms part of the Terms of Service at <https://discountrouter.ai/terms.pdf>. Capitalized terms have the meanings given in those Terms. Customer is responsible for its employees, contractors, applications, and permitted end users. Customer must not knowingly enable, facilitate, conceal, or supply prohibited activity through another person or service.

This AUP supplements, and does not expand the uses permitted by, Section 14 of the Terms. Ordinary internal business use and bona fide embedded applications remain permitted only within that section's boundaries.

2. No model routing, token resale, or access brokering

Do not use DiscountRouter as an upstream provider for third-party model routers, aggregators, model marketplaces, general-purpose model APIs, proxies, relays, or white-label model-access services. Do not supply DiscountRouter-backed model access to another router or reseller, even without a fee or without disclosing DiscountRouter's identity.

Do not sell, resell, rent, lease, sublicense, broker, trade, or redistribute API keys, accounts, tokens, token allowances, credits, quotas, model usage, or inference capacity. Do not operate group buys, shared-capacity pools for unrelated parties, token exchanges, access memberships, or reimbursement arrangements that provide prohibited access. A markup is not required for conduct to be prohibited.

Do not disguise a prohibited arrangement through a thin user interface, rebranding, intermediaries, a bundled subscription, or a different billing unit. Permitted applications must provide distinct functionality and must not give end users DiscountRouter credentials, transferable balances, or independent access to the underlying capacity. These restrictions do not prohibit internal gateways used solely on Customer's behalf or the sale of a finished work product generated through otherwise permitted use.

3. Account, credit, and promotional abuse

Do not share credentials with unauthorized people, expose keys in public repositories or public client-side code, use stolen or compromised credentials, or access another Customer's data, account, or capacity. Keep credentials secured and promptly report suspected compromise.

Do not create or acquire accounts, fabricate identities, conceal common control, or use unrelated organizations to evade eligibility rules, verification, restrictions, or enforcement. Do not continue suspended activity through replacement accounts or other parties.

Do not farm trial credits, referral rewards, discounts, coupons, or promotional allowances through duplicate identities, self-referrals, fabricated activity, or other misrepresentations. Do not exploit balance, refund, or crediting errors; promptly report suspected material errors rather than using them for further unauthorized consumption.

4. Metering, limits, payments, and infrastructure

Do not evade authentication, quotas, rate or concurrency limits, spending caps, provider restrictions, geographic controls, or safety measures. Do not rotate accounts, keys, networks, or intermediaries to defeat such controls or aggregate allowances beyond the applicable entitlement.

Do not falsify, suppress, tamper with, or exploit metering, usage reporting, billing records, caching, retries, cancellations, or error handling to obtain unpaid usage or pricing benefits to which you are not entitled. Do not use stolen payment instruments, submit knowingly false refund or chargeback claims, or intentionally consume Services without authorization to pay. Good-faith billing disputes and legally protected payment-dispute rights remain available.

Do not knowingly overload or impair the Services, monopolize shared resources, maintain wasteful connections for disruption, generate abusive retry loops, or interfere with other Customers or upstream infrastructure. Follow documented retry and backoff instructions. Load, stress, denial-of-service, or resource-exhaustion testing requires prior written authorization from DiscountRouter and authorization for any other affected systems. Legitimate automated applications and ordinary traffic within applicable limits are not prohibited merely because they are automated.

5. Security abuse and platform extraction

Do not distribute malware, ransomware, spyware, or credential-stealing code; conduct phishing, credential theft, unauthorized scanning, exploitation, denial-of-service attacks, or unauthorized access; or materially facilitate these activities.

Do not extract or attempt to obtain non-public platform secrets, credentials, other Customers' information, provider accounts, or capabilities not enabled for your account. Do not scrape non-public service data or misuse confidential platform information to build a competing routing service. Do not defeat access controls or model safeguards to carry out prohibited conduct.

Authorized, good-faith security testing and lawful interoperability remain subject to the Terms, applicable law, and the authorization's scope. Authorization for your own application does not authorize attacks or disruptive testing against DiscountRouter or an upstream provider. Report vulnerabilities responsibly to sales@discountrouter.ai without retaining, exploiting, or disclosing unrelated data. Nothing in this AUP restricts rights that cannot lawfully be restricted.

6. Unlawful, deceptive, and harmful conduct

Do not commit, facilitate, solicit, or materially assist unlawful conduct. Do not use the Services for scams, identity theft, fraudulent transactions, forged documents intended for unlawful conduct, deceptive impersonation for unlawful gain or harm, unsolicited abusive bulk messaging, or coordinated harassment.

Do not create or facilitate child sexual abuse material, non-consensual sexual exploitation, human trafficking, credible threats of violence, or instructions intended to facilitate imminent violent wrongdoing.

Do not knowingly infringe or misappropriate copyrights, trademarks, trade secrets, publicity rights, or other intellectual property. Do not misrepresent affiliation with, endorsement by, or authorization from DiscountRouter or a model provider.

7. Privacy, confidential information, and high-impact uses

Do not unlawfully collect, expose, identify, track, infer, or process personal, confidential, biometric, financial, authentication, or other protected information. Submit only information you are authorized to have processed by DiscountRouter and the applicable request recipients.

For employment, lending, housing, insurance, healthcare, education, legal services, critical infrastructure, public safety, or other regulated or consequential uses, Customer is responsible for applicable law, testing, human review, notices, appeals, recordkeeping, and safeguards. Do not claim DiscountRouter has approved, certified, or validated a regulated use unless it has expressly done so in writing.

8. Provider restrictions and restricted access

Comply with lawful restrictions applicable to the selected model and with applicable export controls, sanctions, and trade restrictions. Do not conceal a prohibited recipient or location, misrepresent an eligible use, or relay restricted traffic through another account, region, organization, or provider to evade a restriction.

Do not use an intermediary to conceal activity prohibited by these Terms or the applicable provider requirements. DiscountRouter may enforce provider requirements where reasonably necessary to maintain access or legal compliance. Ordinary internal tools and privacy-protective networking are not prohibited unless used to evade applicable restrictions.

9. Customer safeguards and cooperation

Maintain reasonable application access controls and safeguards proportionate to your use, protect credentials, and take reasonable steps to prevent prohibited use through your account. Promptly stop known abusive traffic, contain compromised access, and notify DiscountRouter of material misuse or credential compromise.

Provide accurate and reasonably necessary account, business-use, or technical information when requested for a proportionate security or abuse inquiry. Do not destroy or falsify relevant records to obstruct an investigation. This obligation does not require disclosure of unrelated personal information, third-party secrets, or prompt and response content contrary to the applicable Privacy Policy or DPA.

10. Enforcement and review

DiscountRouter may investigate suspected violations and take proportionate protective action, including throttling traffic, restricting a model, disabling credentials, requiring corrective measures or verification, suspending affected accounts, or terminating access as provided in the Terms. It may preserve relevant operational records only as permitted by the Privacy Policy, applicable DPA, and law.

Where circumstances permit, DiscountRouter will attempt to provide notice and an opportunity to address the issue. Immediate protective action may be necessary for serious security threats, fraud, unlawful activity, sanctions concerns, prohibited resale or routing, material provider violations, or ongoing disruption. Termination and any applicable cure rights remain governed by the Terms.

Customer may request review at sales@discountrouter.ai. Access may be restored when the issue is resolved and the relevant risk has been addressed. Fees, credits, refunds, and good-faith billing disputes remain governed by the Terms, applicable order form, and law; this AUP does not impose automatic fines or automatic forfeiture of all balances.

These use restrictions do not expand DiscountRouter's rights to retain or repurpose prompt or response content, change its privacy commitments, or constitute a promise that every request is monitored or every abusive act will be detected.

11. Updates and contact

Updated September 17, 2026. Changes apply prospectively and remain subject to the notice and amendment requirements in the Terms and any applicable signed agreement. Publication alone does not override signed commitments or mandatory legal requirements.

Report suspected abuse, security issues, or enforcement concerns to sales@discountrouter.ai. Include relevant account identifiers and technical details where appropriate; do not include passwords, API secrets, or unnecessary personal information.