X2PROXY

Acceptable Use Policy

Effective date (entry into force): August 1, 2026

Service operator: the x2proxy brand and the person(s) actually performing the administration, support, compliance control and provision of access to the x2proxy service, pending possible incorporation and/or publication of other official identification (the “Provider”).

Contacts: privacy@x2proxy.com — privacy matters and legally significant notices; support@x2proxy.com — support, including payment, refund and abuse-related matters; support chat — https://t.me/x2proxysupport; official channel — https://t.me/x2proxy.

User: a natural person, sole proprietor, legal entity or other person using the x2proxy service (the “User”).

This Acceptable Use Policy (AUP) defines the permitted and prohibited ways of using the x2proxy service, including use through the interface, the API, sub-accounts, internal teams and other integrations.

Use of the Service constitutes the User's agreement to comply with this Policy together with the Terms of Use, the Privacy Policy and the Refund Policy.

The Provider may update this Policy. An updated version takes effect on the date specified in it or upon publication in the Service, unless otherwise required by mandatory law.

1. GENERAL PROVISIONS

1.1. Purpose and status of the Policy

1.1.1. This Acceptable Use Policy (AUP) establishes mandatory rules and restrictions on the use of the x2proxy service.

1.1.2. The Policy applies to all ways of using the Service, including the personal dashboard, the API, sub-accounts, internal teams, automated tools and other integrations.

1.1.3. This Policy is an integral part of the Terms of Use and applies together with the Privacy Policy and the Refund Policy.

1.2. Acceptance of the Policy

1.2.1. Registering an account, topping up the balance, creating proxy configurations, using the API or actually using traffic constitutes acceptance of this Policy.

1.2.2. If the User does not agree with this Policy, the User must refrain from using the Service.

1.3. General model of response measures

1.3.1. Where a risk or violation is identified, the Provider may apply a temporary suspension, freeze, restriction of features, or revocation of access to particular domains, ports, locations or other Service capabilities.

1.3.2. Permanent termination of access is governed by the Terms of Use and may be applied in cases of material or repeated violations.

1.3.3. In cases involving security, abuse, complaints, or payment or compliance risks, measures may be applied without prior notice.

2. GENERAL PRINCIPLES OF USE

2.1. Lawfulness and good faith

2.1.1. The User must use the Service only for lawful purposes and with regard to applicable law, the rules of target resources and obligations towards third parties.

2.1.2. The User independently assesses the lawfulness of its use case, the legitimacy of access to data and the permissibility of automation in relation to specific resources.

2.1.3. Use of the Service must not cause financial, technical, legal or reputational harm to the Provider, other users or third parties.

2.2. Dynamic nature of permitted scenarios

2.2.1. The list of acceptable scenarios set out in this Policy is illustrative, non-exhaustive and may be supplemented, clarified or restricted in light of the development of the Service, risks and the requirements of applicable law.

2.2.2. The fact that a particular use case is not expressly listed among the examples of acceptable use does not make it automatically prohibited; however, such a use case must comply with this Policy, the Terms of Use and applicable law.

2.3. Right to assess risk

2.3.1. The Provider may assess the nature of the use of the Service, the tools employed, the load profile, the target resources and other relevant circumstances for anti-abuse, security and compliance purposes.

2.3.2. Formal compliance with one of the permitted scenarios does not preclude a restriction of access if the specific implementation of the use case creates a risk of abuse, infrastructure blocking, breach of law or infringement of third-party rights.

3. PROHIBITED USE

3.1. General prohibition

3.1.1. The User is prohibited from using the Service for unlawful, malicious, unfair, misleading or otherwise unacceptable activity.

3.1.2. Any use aimed at concealing unlawful activity, circumventing mandatory restrictions or creating material risk for the Provider or third parties is prohibited.

3.2. Network attacks and unauthorized access

3.2.1. DDoS attacks, stress testing without proper authorization, brute force, credential stuffing, password guessing, exploitation of vulnerabilities, circumvention of authentication, circumvention of anti-fraud mechanisms and other forms of unauthorized access are prohibited.

3.3. Malicious and deceptive activity

3.3.1. Malware, botnets, phishing, impersonation, social engineering, ad fraud, click fraud, fake impressions, payment fraud, the creation or support of fraudulent schemes and other forms of deceptive conduct are prohibited.

3.4. Unlawful data collection

3.4.1. The collection of personal data without a proper legal basis, scraping of non-public data, circumvention of authorization, harvesting of credentials, mass collection of email addresses and phone numbers, and the collection of special categories or other sensitive data without lawful authority are prohibited.

3.5. Spam and unwanted communications

3.5.1. Use of the Service for mass mailings, spam, unsolicited messaging, comment spam, direct message spam and other unauthorized communications is prohibited.

3.6. Circumvention of restrictions and abuse of platforms

3.6.1. Circumvention of rate limits, API limits, paywalls, licenses, mandatory geographic restrictions, anti-bot protections and other technical or contractual restrictions is prohibited where such actions are prohibited by applicable law, the rules of the target service or this Policy.

3.6.2. The creation or use of fake personas, networks of fake accounts, artificial-demand schemes, unfair automation of social platforms, marketplace manipulation, ticket scalping, sneaker bots and similar schemes is prohibited.

3.7. High-risk and sensitive areas

3.7.1. Use of the Service for unlawful targeting or abuse against government resources, educational institutions, financial services, fintech platforms and medical systems, or for political influence operations or other sensitive areas, is prohibited where it violates the law, infringes the rights of third parties or creates unacceptable risk.

3.8. Sanctions and export control

3.8.1. Use of the Service to circumvent sanctions, export restrictions, or prohibitions on providing services to certain persons, territories or categories of activity is prohibited where such restrictions apply.

3.9. Materially similar violations

3.9.1. Any activity that is essentially similar to the actions listed above and creates comparable risk of abuse, blocking, legal claims or damage is also prohibited.

4. PERMITTED USE

4.1. Examples of acceptable scenarios

4.1.1. Subject to compliance with this Policy, the following are permitted in particular: lawful public web scraping, SEO monitoring, market research, price monitoring, QA/testing, ad verification, brand protection, research and analytical tasks, software development and other good-faith scenarios.

4.1.2. Use of the Service through the API, sub-accounts, automated tools and the User's internal workflows is permitted, provided that such use remains controlled and lawful and does not violate this Policy.

4.2. Internal use and team

4.2.1. The User may use the Service for its own purposes and grant access to employees, contractors and members of its team, provided that such access is exercised on behalf of and under the control of the User.

4.2.2. The User is responsible for the actions of persons to whom it has granted access to the account, sub-accounts, API keys or other credentials.

4.3. Conditions of acceptability

4.3.1. Any formally acceptable scenario ceases to be considered acceptable if it violates the law or the terms of target services, breaches data-protection requirements, creates abnormal load, is aimed at circumventing restrictions or otherwise falls within the prohibited actions.

5. AUTOMATION AND LOAD

5.1. Controlled automation

5.1.1. The use of scripts, bots, automated clients and other means of automation is permitted only with a controlled load profile, compliance with the rules of target services and the absence of prohibited actions.

5.1.2. The User must itself limit the frequency of requests, avoid sharp spikes in activity, and adjust the behavior of its automation in light of the technical and contractual restrictions of target platforms.

5.2. Limitation of the right to unconditional automation

5.2.1. The presence in the Service description of statements about high performance, concurrency or other technical capabilities does not mean that the User has an unconditional right to use any load profile in any volume and for any purpose.

5.2.2. The Provider may restrict concurrency, request rate, geographic combinations, access to domains, ports and other usage parameters where necessary for anti-abuse, protection of the infrastructure, compliance with the law or fulfilment of third-party requirements.

5.3. Higher-risk automation

5.3.1. The Provider may at any time restrict or prohibit a particular automation pattern if it creates elevated load, increases the risk of infrastructure blocking, is used to circumvent protective mechanisms, or otherwise becomes incompatible with this Policy.

6. LOCATIONS, PORTS AND OTHER TECHNICAL RESTRICTIONS

6.1. General provisions

6.1.1. The Provider may dynamically introduce restrictions on locations, ports, connection categories, types of proxy configurations, access methods and other technical parameters of the Service.

6.1.2. Such restrictions may be introduced for reasons of security, compliance, abuse prevention, technical resilience, risk management or other operational reasons.

6.2. Dynamic nature of restrictions

6.2.1. The availability of particular countries, regions, cities, domains, ports and other technical parameters is not guaranteed and may change at any time.

6.2.2. The User may not circumvent such restrictions by manipulating settings, using multiple accounts, concealing use-case information or by other similar means.

7. RESTRICTED RESOURCES, PORTS AND USE-CASE REVIEW

7.1. Default access and specific restrictions

7.1.1. The basic Service model provides a standard set of available features and destinations. Certain domains, resources, categories of resources, ports or other capabilities may be restricted by default.

7.1.2. Having an account and a paid traffic package does not entail an automatic right of access to all domains, ports and configurations.

7.2. Request to open access

7.2.1. If the User needs access to a restricted resource, domain or port, it may submit a corresponding request to the Provider.

7.2.2. Review of the request may include completion of KYC through a third-party service, a description of the intended use case, indication of specific domains or ports, and the provision of additional explanations at the Provider's request.

7.3. Refusal to undergo verification

7.3.1. A refusal to undergo KYC or to provide use-case information does not, in itself, make the User a violator of this Policy.

7.3.2. However, in that case the Provider may decline to open access to the relevant restricted resources, ports or features.

7.4. Decision and revocation of access

7.4.1. The decision to grant, partially grant, restrict or revoke access to restricted resources is made by the Provider following a risk review and a use-case review.

7.4.2. Access granted may subsequently be reviewed, restricted or revoked upon a change in the level of risk, detection of violations, receipt of complaints, changes to compliance requirements or for other justified reasons.

8. RESALE, EXTERNAL CLIENTS AND INTERNAL SUB-ACCOUNTS

8.1. General rule

8.1.1. The User is prohibited from reselling the Service, providing external client access to it, using the Service on a white-label basis, or otherwise providing it to third parties as a standalone service without the Provider's prior written permission.

8.1.2. Use of the Service within the User's own organization, including employees, contractors and internal sub-accounts, is not considered resale, provided that such access does not turn into a separate external service for third parties.

8.2. Permitted resale

8.2.1. The Provider may, at its discretion, grant written permission for particular resale or partner-use models.

8.2.2. Where such permission is granted, the User undertakes to control end users, ensure compliance with this Policy and respond promptly to reports of violations.

8.3. Revocation of permission

8.3.1. The Provider may revoke a previously granted permission for resale or partner use if a breach of terms, elevated risk, unethical use, or disregard of the agreed restrictions by the User or its clients is identified.

9. MONITORING, COMPLAINTS AND INVESTIGATIONS

9.1. Monitoring of use

9.1.1. The Provider may monitor use of the Service to the extent necessary for security, anti-abuse, compliance, infrastructure stability and protection of the Provider's legitimate interests.

9.1.2. Such monitoring may rely on technical logs, billing/usage anomalies, risk signals, KYC/review outcomes, support tickets, complaints, payment/compliance signals and other relevant sources.

9.1.3. This Policy does not mean that the Provider stores the content of user traffic; monitoring is limited to technical and operational data to the extent necessary for the functioning of the Service and protection of the infrastructure.

9.2. Complaints and external signals

9.2.1. The Provider may take into account complaints and signals from affected persons, target services, rights holders, payment, compliance, security, network and other relevant providers, as well as from competent authorities.

9.3. User cooperation

9.3.1. The User must cooperate in good faith in an investigation, including by providing reasonable explanations of the use case, confirming ownership of the account, responding to security and incident requests, and providing other necessary information within a reasonable time.

10. ENFORCEMENT MEASURES AND AUTOMATED SIGNALS

10.1. List of possible measures

10.1.1. In response to a risk or violation, the Provider may apply a warning, a temporary account freeze, a restriction of particular features, blocking of certain locations, domains or ports, a requirement for additional verification, revocation of previously opened access, or other proportionate measures.

10.2. Automated signals

10.2.1. The Provider may use automated signals, risk scoring and anomaly detection for the initial identification of violations or risks.

10.2.2. Where the nature of the situation or applicable law requires additional safeguards, materially significant restrictions are subject to subsequent manual review or other additional assessment.

10.3. Consequences of violations

10.3.1. A breach of this Policy may result in the application of measures without compensation to the User for losses, loss of traffic or other consequences arising in connection with the User's own violation, and may affect the right to a refund under the Refund Policy.

11. POLICY UPDATES AND ORDER OF PRECEDENCE OF RULES

11.1. Updates

11.1.1. The Provider may update this Policy in light of the development of the Service, changes in risks, legal requirements, complaints and other relevant practice.

11.1.2. An updated version takes effect on the date specified in it or upon publication in the Service, unless otherwise required by mandatory law.

11.2. Precedence of prohibitions

11.2.1. In interpreting this Policy, the provisions on prohibited actions and restrictions prevail over the examples of acceptable use, unless the text expressly provides otherwise.

11.3. Mandatory law

11.3.1. Nothing in this Policy limits the User's mandatory rights that cannot be limited by applicable law.