

# Acceptable Use Policy (AUP)

**Effective Date:** January 2026

**Last Updated:** January 2026

## 1. Purpose and Scope

This **Acceptable Use Policy** (“AUP”) establishes the rules, standards, and expectations for the responsible use of network resources, infrastructure, and related services provided by **NetLir LTD** (“NetLir”, “we”, “our”, “us”).

It forms an integral part of the **Terms of Service** and is binding on all Clients and users of NetLir’s services.

### 1.1. Purpose

The purpose of this Policy is to:

- promote **lawful, ethical, and secure use** of Internet resources managed by or through NetLir;
- protect the **stability, availability, and reputation** of our network and the RIPE NCC ecosystem;
- ensure compliance with applicable **laws, industry standards, and RIPE NCC policies** governing the allocation and management of Internet number resources;
- define acceptable and prohibited activities in relation to IP address space, ASN, and related technical or administrative operations.

This Policy is designed to prevent network abuse, ensure operational continuity, and maintain the trust of clients, partners, and the Internet community.

### 1.2. Scope of Application

This Policy applies to:

- all **clients, customers, and end-users** who purchase, lease, manage, or use IP address space, ASN, or related services provided or sponsored by NetLir;
- all **affiliates, agents, and representatives** acting on behalf of a Client; and
- any **third parties** accessing or transmitting traffic through NetLir’s assigned network infrastructure.

The Policy governs all uses of:

- IPv4 and IPv6 address blocks allocated or assigned by NetLir;
- autonomous system numbers (ASNs) sponsored or managed by NetLir;
- NetLir’s hosting, routing, and LIR management services;
- all communications conducted through NetLir-managed systems or via associated resources.

### 1.3. Legal Foundation

This Policy is based on and aligned with:

- the **UK Communications Act 2003**, **Computer Misuse Act 1990**, and other applicable UK legislation;
- the **RIPE NCC Terms and Conditions** and **RIPE Policies**;
- international Internet governance standards and best practices for responsible network management.

Compliance with this AUP is **mandatory**.

Violation of this Policy may lead to **service suspension, termination, or escalation to RIPE NCC or law enforcement authorities**.

## 2. General Principles

By accessing or using the services provided by **NetLir LTD** (“NetLir”, “we”, “our”, “us”), you agree to adhere to the following core principles of lawful, responsible, and cooperative network use.

### 2.1. Compliance and Accountability

You must:

- **comply** at all times with this Acceptable Use Policy (AUP), the **Terms of Service**, and all applicable **laws, regulations, and RIPE NCC policies**;
- ensure that any use of the services is **lawful, transparent, and consistent** with the intended technical and business purposes;
- maintain accurate organizational and contact details in all **RIPE NCC database objects**, including organisation, inetnum, route, and mntner records;
- provide **timely responses** to compliance or abuse-related requests from NetLir or RIPE NCC.

Failure to cooperate with reasonable compliance checks may result in temporary service suspension.

### 2.2. Responsible Use of Internet Resources

All IP address space, AS Numbers, and related objects provided or sponsored by NetLir must be used **only for legitimate, ethical, and operationally sound purposes**, including:

- lawful network connectivity and routing;
- internal infrastructure or customer services consistent with declared justification;
- public Internet operations that respect accepted network and security standards (RFC 1918, RFC 2050, RIPE-731, etc.).

You must not use NetLir’s services to facilitate, conceal, or support any unlawful or abusive activity.

### 2.3. Integrity and Network Stability

You are required to use NetLir’s resources and services in a manner that:

- does **not disrupt or degrade** the performance, availability, or security of NetLir’s network, or of the global Internet routing system;
- avoids the transmission of malformed, spoofed, or malicious network traffic;
- respects routing best practices (e.g., **RPKI validation, prefix length standards, anti-spoofing filters**);
- prevents IP space from being **blacklisted, hijacked**, or associated with recurrent abuse.

Clients must immediately notify NetLir of any security incident, abuse report, or blacklisting event related to their resources.

## 2.4. Responsibility for Delegated Use

The Client bears **full responsibility** for all actions performed using its assigned IP addresses, ASNs, or delegated resources — including those of its:

- employees, partners, or contractors;
- resellers, downstream customers, or hosted networks.

If a subcontractor or downstream entity engages in prohibited activity, NetLir may hold the primary Client accountable and take corrective action under Section 5 (Monitoring and Enforcement).

## 2.5. Cooperation with NetLir and RIPE NCC

You agree to:

- cooperate fully with **NetLir, RIPE NCC**, and relevant authorities in the investigation of abuse or policy breaches;
- provide required documentation (e.g., **network diagrams, justification of usage, LOA**) when requested;
- ensure ongoing compliance with the latest **RIPE community policies**.

Non-cooperation or repeated policy violations may result in resource revocation or termination of services.

## 3. Prohibited Activities

Clients must not use, or permit others to use, any service, network, or resource provided by **NetLir LTD** for any unlawful, abusive, or harmful purpose.

Engaging in or promoting the following activities constitutes a **material breach** of the Terms of Service and may result in **immediate suspension or termination without refund**.

### 3.1. Network Abuse

You may not:

- initiate, participate in, or facilitate **Denial-of-Service (DoS / DDoS)** attacks against any system or network;

- perform **unauthorized port scans, vulnerability testing, or packet sniffing** on networks or systems without explicit written consent;
- run **open mail relays, recursive DNS resolvers, or proxy servers** that can be abused by third parties;
- use any part of the assigned IP space for **botnets, command-and-control (C2) infrastructure, malware distribution, or phishing toolkits**;
- create **route leaks** or incorrect BGP advertisements that may affect Internet routing stability.

### 3.2. Spam and Unsolicited Communications

You may not:

- send or facilitate the transmission of **unsolicited bulk or commercial email** (“spam”), including messages that advertise illegal or unethical products or services;
- use **harvested, purchased, or automatically generated email lists**;
- send **SMS, VoIP, or instant-messaging spam**;
- forge email headers or use misleading subject lines;
- omit legally required **unsubscribe or opt-out mechanisms** under applicable UK and EU law (e.g., Privacy and Electronic Communications Regulations 2003).

NetLir maintains zero tolerance toward spam abuse. Accounts involved in repeated spam activity may be permanently blacklisted.

### 3.3. Illegal or Unlawful Content

You may not host, store, transmit, or link to any content that violates **UK law, international law, or RIPE NCC policy**, including but not limited to:

- **child sexual abuse material (CSAM)** or any form of exploitation content;
- **terrorist propaganda, hate speech, or incitement to violence**;
- **copyright infringement** or distribution of pirated software, music, or video;
- **fraudulent schemes, identity theft, or impersonation** of individuals or organizations;
- **illegal gambling operations**, pyramid schemes, or unlicensed **financial, crypto, or investment services**;
- **sale of counterfeit goods**, weapons, or controlled substances.

### 3.4. Security and System Violations

You may not:

- attempt to gain **unauthorized access** to systems, accounts, or data belonging to NetLir or any third party;
- bypass or interfere with **authentication, encryption, or access-control mechanisms**;
- deliberately disrupt the **availability or performance** of any system or service;
- deploy **mining software, network scanners, or automation scripts** that cause excessive load or degrade performance;
- use the services to **circumvent IP reputation systems, filtering, or blocklists**.

All Clients must take reasonable measures to secure their infrastructure and promptly mitigate any detected compromise.

### 3.5. Misrepresentation and False Information

You may not:

- provide **false, misleading, or incomplete details** in RIPE NCC database objects, including `organisation`, `inetnum`, or `abuse-c` contacts;
- impersonate another individual or entity in communications or online presence;
- use NetLir's name, logo, or trade identity without **prior written authorization**;
- make any public statement or representation implying that your organization is **affiliated, endorsed, or certified by NetLir** unless explicitly agreed in writing.

### 3.6. Consequences of Violation

Any activity falling under the categories above may result in:

- immediate **suspension or revocation** of IP resources or ASN;
- **null-routing or filtering** of abusive traffic;
- **reporting** to RIPE NCC, law enforcement, or abuse clearinghouses;
- **termination of services** without prior notice or refund.

NetLir reserves the right to determine, at its sole discretion, whether any conduct constitutes a violation of this Policy.

## 4. RIPE NCC and Compliance Obligations

### 4.1. General Compliance

All Clients of NetLir LTD must adhere to the **RIPE NCC policies, procedures, and contractual requirements** governing the use, allocation, and registration of Internet number resources.

These obligations are binding on both NetLir (as a sponsoring LIR) and the Client (as an end user or resource holder).

Clients agree to comply with all applicable documents published by the **RIPE NCC**, including but not limited to:

- **IPv4 Address Allocation and Assignment Policies;**
- **IPv6 Address Allocation and Assignment Policies;**
- **Autonomous System (AS) Number Assignment Policy;**
- **RIPE Database Terms and Conditions;**
- **Abuse Contact Management (abuse-c) Policy;**
- **Transfer and Merger Procedures for Internet Number Resources;**
- **RIPE NCC General Terms and Conditions.**

Use of NetLir's services implies full and continuous compliance with the above.

### 4.2. Documentation and Verification

To ensure compliance, **NetLir** may, at any time, request the Client to provide supporting documentation, including but not limited to:

- valid **company registration** or **personal identification documents** (for individual resource holders);
- **justification of resource usage**, including network topology, infrastructure plans, or service purpose;
- **Letter of Authorization (LOA)** confirming the right to announce or manage specific prefixes;
- **maintainer (mntner)** or **organisation object** references used in the RIPE Database;
- contact information for **technical** and **administrative** representatives.

NetLir reserves the right to **suspend or refuse service activation** until the required documents are verified and approved.

### 4.3. KYC/KYB and Anti-Abuse Screening

As part of NetLir's **Know Your Customer (KYC)** and **Know Your Business (KYB)** procedures, Clients must:

- provide truthful and up-to-date identity and ownership information;
- disclose the **beneficial owner(s)** of the organization (where applicable);
- confirm that the organization and its representatives are **not subject to international sanctions**;
- ensure that all information submitted to the RIPE NCC Database is accurate, lawful, and regularly updated.

False, incomplete, or misleading information constitutes a **material breach** of this Policy.

### 4.4. Cooperation and Audit

Clients must cooperate fully with **NetLir** and **RIPE NCC** in the event of:

- policy compliance checks;
- audits of resource usage or registration data;
- abuse complaints or law enforcement requests.

If the Client fails to respond to reasonable requests for verification within the specified timeframe, NetLir may:

- **suspend access** to the relevant IP space or ASN;
- **reclaim** resources in accordance with RIPE NCC procedures;
- **terminate** the Client's service agreement without liability or refund.

### 4.5. Consequences of Non-Compliance

Failure to comply with RIPE NCC policies, maintain accurate data, or provide required documentation may result in:

- temporary suspension of services or RIPE sponsorship;

- revocation or deregistration of IP addresses or ASNs;
- notification to **RIPE NCC** and relevant authorities;
- permanent **termination of contract** and refusal of future services.

NetLir reserves the right to determine, at its sole discretion, whether a Client is in breach of these obligations.

## 5. Monitoring and Enforcement

### 5.1. Investigation and Oversight

**NetLir LTD** reserves the right to investigate any actual or suspected violation of this Acceptable Use Policy (AUP), the Terms of Service, or RIPE NCC policies.

To ensure compliance and protect the integrity of its network, NetLir may, at its discretion and without prior notice:

- monitor traffic patterns and metadata to detect potential **abuse, spam, or denial-of-service activity**;
- review **RIPE Database objects, WHOIS data, and routing announcements (BGP)** for correctness and consistency;
- perform internal audits or compliance checks on resource usage;
- cooperate fully with **RIPE NCC, law enforcement, and recognized abuse reporting bodies** (e.g. CERT, Spamhaus, Interpol) to address verified incidents;
- request additional documentation or clarification from the Client when suspicious activity is detected.

All monitoring and investigation procedures are conducted strictly in accordance with:

- the **UK Data Protection Act 2018**,
- the **UK GDPR**, and
- NetLir's **Privacy Policy**, ensuring that data is processed only to the extent necessary to maintain network security and legal compliance.

### 5.2. Corrective and Enforcement Actions

If NetLir determines, in its reasonable discretion, that a Client has violated this Policy, any RIPE NCC rule, or applicable law, NetLir may take one or more of the following corrective measures — **with or without prior notice**, depending on the severity and urgency of the violation:

1. **Advisory or Warning Notice** – a written request to cease or remediate the offending activity within a specified period.
2. **Temporary Suspension** – partial or full suspension of services, including deactivation of affected IP prefixes, ASNs, or portal access.
3. **Traffic Mitigation** – implementation of technical controls such as blocking, null-routing, filtering, or rate-limiting specific traffic flows to contain abuse.
4. **Revocation of Resources** – withdrawal of IP address space, ASN sponsorship, or other RIPE-registered objects managed through NetLir.

5. **Reporting Obligations** – formal notification to **RIPE NCC, law enforcement, anti-abuse networks**, or impacted third parties.
6. **Permanent Termination** – full contract termination and blacklisting from future NetLir services.

Repeated, deliberate, or severe violations — including criminal activity, network abuse, or misrepresentation — may result in **permanent termination without refund or reinstatement**.

### 5.3. Restoration of Services

Suspended services may be reinstated only after:

- the Client has **resolved the root cause** of the violation;
- NetLir has verified remediation measures; and
- any applicable **reactivation or administrative fees** have been paid.

NetLir retains sole discretion to determine whether sufficient corrective action has been taken.

### 5.4. Cooperation with Authorities

Where required by law or RIPE NCC policy, NetLir may disclose relevant information to:

- the **Information Commissioner's Office (ICO)**,
- **UK law enforcement agencies**,
- **RIPE NCC**, or
- recognized **abuse coordination networks**.

All disclosures are limited to what is strictly necessary and proportionate to the purpose of the investigation.

## 6. Reporting Abuse

### 6.1. How to Report Abuse

All reports of abuse, security incidents, or suspected violations of this **Acceptable Use Policy (AUP)** should be submitted to the dedicated address:  
**support@netlir.pro**

This mailbox is continuously monitored by NetLir's **Abuse and Compliance Team**. Reports submitted through other channels (e.g., support tickets or social media) may experience delays in processing.

### 6.2. Required Information

To ensure timely and effective investigation, abuse reports **must include sufficient technical detail and evidence**, including:

- **Description of the issue** — a short summary of the observed activity (e.g., spam, DDoS, scanning, phishing, IP hijacking, or illegal content).
- **Source information** — IP addresses, domain names, or ASNs involved in the incident.
- **Timestamps** — clearly indicated and preferably in UTC format.
- **Supporting data** — such as full email headers, log snippets, packet captures, screenshots, or abuse reports from trusted networks.
- **Reporter identification** — your name, organization (if applicable), and contact email for follow-up.

Incomplete or anonymous reports may be deprioritized or closed if insufficient evidence is provided.

### 6.3. Processing and Response Time

NetLir undertakes to:

- acknowledge receipt of valid abuse reports **within 24–48 hours** (business days);
- review and assess the incident severity and policy implications;
- take **appropriate corrective action** as required (e.g., contacting the client, blocking IPs, or notifying RIPE NCC).

Critical incidents — such as **network-wide attacks, malware distribution, or law enforcement alerts** — are handled with **priority** and may result in immediate suspension or null-routing of affected resources.

These response targets are non-binding service targets and do not constitute a Service Level Agreement unless agreed in a separate SLA.

### 6.4. Cooperation with Reporters

Where necessary, NetLir may request additional logs, metadata, or clarification to validate the report.

Reporters are encouraged to cooperate in good faith and preserve relevant technical evidence for at least **seven (7) days** after submission.

### 6.5. Confidentiality and Data Protection

All abuse reports are handled confidentially and in accordance with:

- the **UK Data Protection Act 2018**,
- the **UK GDPR**, and
- NetLir’s internal **Incident Response and Data Retention Policy**.

Personal data shared in abuse reports will only be used for investigation, remediation, or legal compliance and will not be disclosed beyond what is necessary for resolution.

### 6.6. Escalation

If you believe your report has not been properly addressed or involves a systemic issue, you may escalate your complaint by contacting:  
**support@netlir.pro**

For matters related to **RIPE NCC resource management**, you may also contact the **RIPE NCC** directly at <https://www.ripe.net/contact-form>.

## 7. Liability and Responsibility

Clients are fully responsible for:

- all traffic originating from their allocated IP address space;
- ensuring their users and customers adhere to this Policy;
- cooperating with investigations into network abuse or RIPE NCC violations.

NetLir is not liable for any damages, loss, or disruption resulting from enforcement actions or suspension taken in good faith under this Policy.

### 7.2. Indemnification

The Client agrees to **indemnify, defend, and hold harmless** NetLir, its officers, employees, and affiliates from and against any and all **claims, damages, liabilities, costs, and expenses** (including reasonable legal fees) arising from:

- misuse of Internet resources or violation of this Policy;
- non-compliance with **RIPE NCC, UK law**, or international regulations;
- actions or omissions by any **third party** acting through the Client's network or under its control;
- reputational or operational damage caused by blacklisting, abuse, or IP hijacking incidents.

This indemnity remains in effect even after the termination or expiration of the Client's agreement with NetLir.

### 7.3. NetLir's Limitation of Liability

To the maximum extent permitted by law, **NetLir LTD** shall not be liable for:

- any **indirect, incidental, special, or consequential damages**;
- **loss of profits, data, goodwill, or business opportunities**;
- interruptions in connectivity, routing, or service availability;
- enforcement measures taken in **good faith** under this Policy or RIPE NCC compliance obligations;
- consequences of **third-party misuse**, security incidents, or legal actions arising from the Client's activities.

NetLir's total aggregate liability for any claim shall be limited to the amount paid by the Client for the service during the **preceding three (3) months**.

## 7.4. Good Faith Enforcement

All actions taken by NetLir under this Policy — including monitoring, suspension, blocking, or reporting — are carried out in **good faith** for the purposes of:

- protecting the **integrity and security** of the Internet ecosystem;
- ensuring compliance with **RIPE NCC and legal obligations**; and
- preventing harm to other networks, users, or the general public.

Such actions shall not be considered a breach of contract or grounds for any claim against NetLir.

## 8. Policy Updates

### 8.1. Policy Updates

NetLir LTD reserves the right to review, amend, or update this **Acceptable Use Policy (AUP)** at any time to reflect:

- changes in **applicable law or regulatory requirements**;
- updates to **RIPE NCC policies or membership terms**;
- technical or operational developments within NetLir's infrastructure; or
- changes in **industry standards and best practices**.

The most recent and authoritative version of this Policy will always be available on our official website:

<https://netlir.pro>

Any revisions will take effect **upon publication** unless otherwise stated.

Continued use of NetLir's services after such updates constitutes the Client's **acceptance of the revised terms**.

### 8.2. Notification of Changes

Where required by law or at NetLir's discretion, material changes to this Policy may be communicated via:

- email notification to registered account contacts;
- publication in the customer portal; or
- official notice on the NetLir website.

Clients are encouraged to review this Policy periodically to remain informed about their obligations and NetLir's enforcement procedures.

## 9. Contact Information

For questions or clarification regarding this Acceptable Use Policy, please contact:

**NetLir LTD**  
**support@netlir.pro**  
**+44 208 159 8921**