Acceptable Use Policy

Version 2.0, effective 9 November 2026. Earlier versions are available at binadit.com/aup/archive.

1. Scope and Applicability

This Acceptable Use Policy (the "AUP") governs the use of all services supplied by Binadit B.V. ("Binadit", "we", "us", "our"), a company incorporated in the Netherlands (Chamber of Commerce 80923216, VAT NL861852990B01), with its registered office at Seinhuiswachter 2, 3034 KH Rotterdam. The services covered include, without limitation, web hosting, VPS hosting, managed cloud, managed infrastructure, DevOps, colocation, domain registration, email, backup, monitoring and any related professional services (collectively, the "Services").

This AUP applies to every person or legal entity that uses the Services, including our direct customers ("Customer"), any end users, subscribers, visitors, sub-accounts, resellers, employees, contractors and any third party who accesses content or systems provided through the Services (collectively, "Users"). The Customer is responsible for ensuring that all of its Users comply with this AUP and remains fully liable for any breach caused by its Users.

This AUP forms an integral part of the agreement between Binadit and the Customer and must be read together with our Terms and Conditions, Privacy Policy and Data Processing Agreement. In the event of any conflict, the stricter provision protecting the network, users, or third parties shall prevail.

This AUP forms part of the Agreement under Article 7 of Binadit's General Terms and Conditions (binadit.com/terms). Article 8 of the General Terms and Conditions governs notices, suspension and statements of reasons. If this AUP conflicts with the Data Processing Agreement (binadit.com/dpa) regarding personal data, the Data Processing Agreement prevails. Mandatory consumer law and Article 16 of the General Terms and Conditions always prevail.

2. Permitted Use

The Services may only be used for lawful purposes and in a manner that does not infringe the rights of, restrict, or inhibit any third party's use of the internet or Binadit infrastructure. Permitted uses include, but are not limited to: hosting of lawful business websites and applications, running business-grade workloads, sending transactional email within recognised anti-abuse limits, lawful storage and processing of data, and development and testing of software.

3. Prohibited Use

The following categories of use are strictly prohibited. This list is non-exhaustive, and Binadit reserves the right to classify additional activities as prohibited where they create legal, operational, reputational or security risk.

3.1 Illegal Activity

- Any activity that violates Dutch law, European Union law, or any applicable law of the jurisdiction in which the User, Customer, or affected third party is located.
- Violation of economic sanctions, export controls or counter-terrorism financing regulations, including those administered by the United Nations, the European Union, the Netherlands, OFAC, or the United Kingdom. The Services may not be used by, on behalf of, or for the benefit of any sanctioned person, entity, regime or jurisdiction.
- Money laundering, terrorism financing, tax evasion, bribery or any form of financial crime.
- Human trafficking, modern slavery, child labour, or any activity violating fundamental human rights.

3.2 Harmful, Abusive or Malicious Content and Activity

- Distribution, hosting, linking to, facilitation of, or soliciting of Child Sexual Abuse Material (CSAM), non-consensual intimate imagery, or any content sexually exploiting minors. Such content is reported immediately to the relevant authorities (including EOKM / INHOPE) and results in instant termination.

- Content inciting terrorism, violent extremism, genocide, or violence against individuals or groups based on race, ethnicity, religion, nationality, gender, sexual orientation, disability or similar protected characteristics.
- Harassment, stalking, doxing, threats of violence, or targeted intimidation.
- Defamatory, libellous or fraudulent content.
- Content that infringes intellectual property rights, trade secrets, publicity rights or confidentiality obligations, including unauthorised distribution of copyrighted software, media, warez, cracks, keygens or pirated material.
- Counterfeit goods, forged documents, fake identification, fake diplomas, or services that facilitate identity fraud.

3.3 Security Abuse and Network Interference

- Unauthorised access to, scanning of, penetration testing of, or interference with any system, network, or data that the User is not explicitly authorised to test. Authorised penetration testing of the Customer's own systems requires prior written notice to Binadit.
- Distribution or hosting of malware, ransomware, spyware, rootkits, cryptographic miners (without prior written consent), trojans, viruses, worms or botnet command-and-control infrastructure.
- Phishing, smishing, vishing, credential harvesting, fake login pages, or impersonation of any person, brand or government body.
- Denial-of-service (DoS), distributed denial-of-service (DDoS), amplification, reflection, or traffic flooding attacks, whether as source, intermediary or staging point.
- IP address spoofing, BGP hijacking, DNS poisoning, ARP spoofing or any technique that falsifies the origin of network traffic.
- Any use of the Services as an open relay, open proxy, open resolver, or anonymisation layer for unlawful activity.
- Circumventing, disabling or attempting to circumvent any security or access-control mechanism of the Services, other Users, or third-party systems.
- Excessive resource consumption, fork bombs, or patterns of usage that degrade shared infrastructure for other customers.

3.4 Email, Messaging and Spam

- Sending unsolicited bulk or commercial email ("spam"), in violation of applicable anti-spam laws (including the Dutch Telecommunicatiewet, EU ePrivacy Directive, GDPR, CAN-SPAM, CASL).
- Sending email with forged headers, falsified sender information, or without a working unsubscribe mechanism where required.
- Operating mailing lists without verifiable opt-in consent of the recipients.
- Hosting websites or services advertised through spam sent from any network, regardless of whether the spam itself originates from Binadit infrastructure ("spamvertising").
- Sending SMS, push notifications or other messaging in violation of applicable consent and anti-abuse laws.

3.5 Categorically Prohibited Business Categories

The following business categories are not permitted on any Binadit product, plan or infrastructure, regardless of licensing, jurisdiction, age-verification, or prior correspondence. Binadit will not grant exceptions for these categories and will suspend or terminate any account found to be operating in them:

- Adult content of any kind, including pornography, adult entertainment, escort services, cam sites, erotic chat, adult dating or any sexually explicit material - regardless of whether it is legal in the jurisdiction of the Customer or its end users.
- Online gambling, betting, lotteries, casinos, sportsbooks, poker rooms, sweepstakes or games of chance in any form, whether licensed or unlicensed.

- Cryptocurrency mixers, tumblers, privacy coins mixing services or any service designed to obscure the origin, destination or ownership of digital assets.
- Initial Coin Offerings (ICOs), token sales, token generation events, unregistered securities offerings or any unlicensed financial, banking, investment, lending, insurance or payment services.
- Tor exit nodes, public VPN services, public proxy services or any other anonymisation service open to unknown or anonymous third parties.
- IPTV services, cyberlockers, file-sharing services or streaming platforms that distribute, index or link to third-party copyrighted material, whether as a primary or ancillary purpose.

3.6 Other Prohibited and High-Risk Activities

In addition to § 3.5, the following activities are prohibited. Binadit reserves the right to classify additional activities as prohibited where they create legal, operational, reputational or security risk, and to refuse or terminate any such activity at its sole discretion:

- Cryptocurrency mining, high-frequency trading bots or any workload designed to monopolise shared infrastructure.
- Services related to firearms, ammunition, explosives, controlled substances, prescription pharmaceuticals, unlicensed medical devices, or "research chemicals".
- Multi-level marketing, pyramid schemes, Ponzi schemes, "get rich quick" schemes, high-yield investment programs or binary options platforms.
- Services that scrape, store or monetise personal data in violation of the GDPR or other data protection law.
- Generative-AI services producing non-consensual deepfakes, synthetic identity documents, or synthetic CSAM.

4. Compliance with Law and Sanctions

The Customer warrants that its use of the Services at all times complies with: (a) Dutch law; (b) European Union law, including the GDPR, the Digital Services Act, the NIS2 Directive and the ePrivacy Directive; (c) the laws of any jurisdiction from which the Customer operates or to which it directs its services; and (d) all applicable international sanctions and export control regimes. The Customer shall cooperate fully with any investigation or lawful order from a competent authority, and shall indemnify Binadit against any claim, fine, or penalty arising from the Customer's non-compliance.

5. Fraud, Abuse and Harmful Content Prevention

The Customer shall implement reasonable technical and organisational measures to prevent misuse of the Services, including but not limited to: keeping software up to date and patched; using strong authentication and multi-factor authentication where available; segregating privileged accounts; monitoring application logs for abuse; configuring rate limits, CAPTCHA and anti-bot measures on user-generated content forms; and responding promptly to abuse reports.

Where the Customer operates a platform allowing user-generated content, the Customer must provide a clearly abuse-reporting channel, enforce its own terms of service, and take down unlawful content without undue delay upon notification, in line with the Digital Services Act and the notice-and-action procedure.

6. Responsibility for End Users, Sub-Users and Third Parties

The Customer is fully responsible for the acts and omissions of every End User, sub-user, reseller customer, employee, contractor and third party that accesses or uses the Services through the Customer's account or infrastructure, as if those acts or omissions were its own. The Customer shall:

- flow down this AUP (or equivalent obligations no less strict) to all such persons;
- maintain adequate records to identify the source of any abusive content or activity;
- assist Binadit in investigating abuse complaints and provide any information reasonably requested within the deadline set by Binadit;

- accept that Binadit is not responsible for content generated by the Customer's End Users, without prejudice to Binadit's right to act upon that content under this AUP.

7. Monitoring, Enforcement and Remedies

Binadit does not routinely monitor the content of customer traffic or stored data. However, Binadit reserves the right (but has no obligation) to monitor network traffic patterns, system logs, and publicly accessible content where this is necessary to: (a) operate, secure and maintain the Services; (b) investigate suspected violations of this AUP; (c) comply with a court order, subpoena or binding request from a competent authority; (d) respond to an abuse report; or (e) protect the rights, property, safety, or reputation of Binadit, its customers, or third parties.

Where Binadit reasonably suspects a violation of this AUP, Binadit may, at its sole discretion and without prior notice, take any or all of the following actions:

- issue a warning and request remediation within a stated deadline;
- block specific traffic, IP addresses, ports, or domain names;
- null-route, filter, or rate-limit traffic;
- remove, disable access to, or quarantine unlawful or abusive content;
- suspend the Services in whole or in part;
- terminate the Services and the underlying agreement with immediate effect, without refund, in the case of serious, repeated, or irreparable violations;
- preserve and disclose data to law enforcement, regulators, or affected third parties where legally required or justified by a legitimate interest; and
- invoice the Customer for any costs reasonably incurred by Binadit as a result of the violation, including abuse-handling costs, legal fees, and third-party claims.

Violations involving CSAM, imminent threats to life or critical infrastructure, active attacks against third parties, or legally mandated takedowns will result in immediate suspension without prior notice. Binadit will notify the Customer as soon as reasonably practicable thereafter, unless prohibited by law or by a competent authority.

When Binadit takes a measure under this AUP, it gives the Customer a clear and specific statement of reasons, as required by Article 17 of the Digital Services Act (Regulation (EU) 2022/2065), unless the law prohibits this. The statement explains which measure was taken, its scope and duration, the facts relied on, and why the content or use is considered illegal or contrary to this AUP. The Customer may object by e-mail to abuse@binadit.com; Binadit then reviews its decision. The Customer may also go to court.

"Termination without refund" does not apply to Consumers to the extent mandatory consumer law grants a refund. For Consumers, Article 16 of the General Terms and Conditions applies.

8. Reporting Abuse

Suspected violations of this AUP, unlawful content hosted on Binadit infrastructure, or security incidents involving Binadit IP space can be reported to abuse@binadit.com.

To allow us to act on a notice about illegal content, please include:

1. a sufficiently substantiated explanation of why you consider the content illegal or contrary to this AUP;
2. the exact location of the content, such as the URL, IP address or domain name;
3. your name and e-mail address, except for notices about child sexual abuse material;
4. a statement that you believe in good faith that the information in your notice is accurate and complete; and
5. where available, timestamps with time zone and relevant logs.

Binadit confirms receipt without undue delay, handles notices in a timely, diligent, non-arbitrary and objective manner, and informs you of its decision and of the possibilities for redress.

9. Changes to this Policy

Binadit may amend this AUP in accordance with Article 17 of the General Terms and Conditions. Amendments apply immediately to new customers and to existing customers 30 days after notification by e-mail. If an amendment materially disadvantages the Customer, the Customer may terminate the affected Agreement free of charge with effect from the date it takes effect.

10. Contact

Binadit B.V.
Seinhuiswachter 2
3034 KH Rotterdam
The Netherlands
General: contact@binadit.com
Abuse: abuse@binadit.com
Phone: +31 10 477 5362
Single point of contact for authorities and users under the Digital Services Act: contact@binadit.com (Dutch and English).