Acceptable Use Policy

Effective date: 28 July 2026

This Acceptable Use Policy (hereinafter — the "Policy") establishes the rules for using the services provided by **UPHOST SOLUTIONS LIMITED** (Company number 17188833), hereinafter — the "Company". The Policy is binding on all clients (hereinafter — the "Client") and is aimed at ensuring the lawfulness, security and stability of the infrastructure. The Policy forms an integral part of the Company's Terms of Service (public offer). By using the Company's services, the Client confirms their agreement with this Policy.

1. General Provisions

1.1. The Client must use the services responsibly, without violating the rights and interests of other users and without creating a threat to the stability and security of the platform.

1.2. The Client must comply with applicable laws, regulations and international standards, including the laws of the United Kingdom (including the Computer Misuse Act 1990, the Fraud Act 2006, the Online Safety Act 2023 and the Privacy and Electronic Communications Regulations 2003), as well as the laws of the country of the Client's location and the country where the servers are located.

1.3. The Client is independently responsible for protecting their data, accounts and software, including the use of up-to-date updates and appropriate information security measures.

1.4. The Client is responsible for all content and activity carried out using their services, including by third parties who have gained access to the Client's services (including in cases of compromise).

1.5. If security incidents or suspicious activity are detected, the Client must immediately notify the Company's support service at support@uphost.cloud.

2. Prohibited Activities

2.1. Using the services for purposes contrary to the law and the Company's terms of service, as well as any of the activities listed below, is prohibited.

2.2. Spam and Mailing Abuse

2.2.1. Bulk sending of messages (e-mail, SMS, messages in messengers and social networks) without the prior express consent of the recipients; sending spam of any kind.

2.2.2. Using purchased, rented or automatically harvested contact lists.

2.2.3. Sending messages with forged, hidden or misleading headers, sender addresses or subjects.

2.2.4. Hosting and operating open mail relays, open proxy servers and anonymous bulk mailing services.

2.2.5. Advertising resources hosted with the Company by means of spam sent from any infrastructure (spamvertising).

2.3. Malicious Software

2.3.1. Creating, storing, distributing or running malicious software of any kind: viruses, trojans, worms, ransomware, spyware, rootkits, keyloggers.

2.3.2. Hosting and operating botnet command-and-control servers (C&C/C2), malware control panels and malware distribution infrastructure; participation in botnets, including as a result of the Client's failure to remedy a

compromise.

2.4. Phishing and Fraud

2.4.1. Phishing — creating, hosting or distributing fake web pages, forms and messages imitating legitimate organisations for the purpose of obtaining credentials, payment or other confidential information.

2.4.2. Spoofing of domain names, e-mail addresses and other identifiers; pharming.

2.4.3. Fraud of any kind (including acts falling under the Fraud Act 2006), identity theft, transactions with stolen payment data (carding), financial pyramids.

2.4.4. Registration using false information.

2.5. Network Attacks and Unauthorised Access

2.5.1. Carrying out DDoS attacks of any type and facilitating them, including hosting attack tools (stressers, booters).

2.5.2. Scanning of third parties' ports and networks, password brute-forcing, exploitation of vulnerabilities, unauthorised access and attempts to access other people's systems and data in violation of the Computer Misuse Act 1990.

2.5.3. Interception, substitution and monitoring of other people's network traffic; IP spoofing; forging network packets and routing information.

2.5.4. Penetration testing is permitted solely in relation to the Client's own systems or with the written consent of the owner of the system being tested.

2.6. Illegal and Prohibited Content

2.6.1. Hosting or distributing illegal, copyright-infringing, deceptive or defamatory content.

2.6.2. Hosting child sexual abuse material (CSAM) and any sexual material involving minors — entails immediate termination of the services and referral of the information to law enforcement authorities.

2.6.3. Hosting pornography, including links and advertisements containing pornographic scenes.

2.6.4. Hosting content promoting terrorism and extremism, containing calls to violence or inciting hatred; doxxing and violation of third parties' privacy.

2.6.5. Hosting unlicensed software, pirated copies of works and means of circumventing technical protection in violation of the Copyright, Designs and Patents Act 1988.

2.6.6. Illegal trade in: drugs, weapons, stolen data, forged documents and other items whose circulation is prohibited or restricted by law; organising illegal gambling.

2.7. Other Prohibited Activities

2.7.1. Prolonged use of allocated resources (CPU, RAM, I/O) at a level that threatens the normal operation of other clients.

2.7.2. Cryptocurrency mining without the Company's prior written consent.

2.7.3. Hosting network scanners, proxy checkers and similar software, as well as services (including those with paid or private access) that may serve as auxiliary means for unlawful activities on the Internet.

2.7.4. Using the services to create, provide or sell commercial VPN services, including paid, public or mass access for third parties; the use of a VPN for the Client's personal, non-commercial purposes is permitted.

2.7.5. Actions capable of damaging the Company's reputation or infrastructure, including actions resulting in the Company's IP addresses being blacklisted (RBL/DNSBL).

2.7.6. Use of the services by persons and organisations included in sanctions lists (United Kingdom/OFSI, OFAC, EU, UN, etc.), or in the interests of such persons.

2.7.7. Reselling the Company's services without its written consent; where consent has been given, the Client is responsible for compliance with this Policy by its end users.

3. Resource Usage

3.1. Virtual servers use shared computing capacity distributed among clients. Short-term load peaks are permitted; however, constant utilisation of all vCPUs at 100% is not permitted.

3.2. Exceeding limits: if the Client's load systematically exceeds the norms established by the tariff, the Company may limit resources, offer an upgrade to a higher tariff or take other measures to restore stable operation.

3.3. Lack of response: if the Client ignores the Company's requests to reduce the load, the Company may unilaterally restrict or block the server until the violations are remedied.

3.4. The use of disk and network resources must remain within reasonable limits. For high-load applications, the implementation of caching and optimisation is recommended.

4. Network Traffic

4.1. Excessive use of traffic that adversely affects the operation of the network and other clients is prohibited. To ensure comfortable operation for all clients, the Company applies a Fair Use Policy.

4.2. If the permissible norms are exceeded, bandwidth may be limited (shaping) to 10–100 Mbit/s, depending on the tariff, until the end of the billing period.

4.3. The Company reserves the right to monitor network activity (volume, intensity and directions of traffic, without systematic review of the content of the Client's data) to ensure compliance with this Policy.

5. E-mail and Anti-Spam

5.1. To protect against abuse, outgoing SMTP ports (25, 465) are closed by default.

5.2. Ports may be opened upon request to the support service after additional verification.

5.3. The Client must maintain correct SPF, DKIM and DMARC records and comply with mailing legislation (recipients' consent, a working opt-out mechanism), including the Privacy and Electronic Communications Regulations 2003 (PECR).

5.4. The blacklisting (RBL/DNSBL) of the Company's IP addresses through the Client's fault constitutes a material breach of this Policy.

6. Contact Details

6.1. The Client must provide accurate and up-to-date contact details upon registration and use them for communication.

6.2. The use of temporary or disposable e-mail addresses is prohibited.

6.3. Contact information must be updated within 7 (seven) days of any change.

6.4. Messages sent by the Company to the e-mail address specified by the Client are deemed proper notice to the Client.

7. Security and Incident Response

7.1. If the services are compromised or involved in violations, the Company may suspend or restrict their operation, notifying the Client where possible.

7.2. The Client must promptly remedy vulnerabilities, remove malware and prohibited content, reinstall software and change credentials at the Company's request.

7.3. The Client must cooperate in incident investigations and provide the necessary data within the limits established by law.

7.4. The Company may disclose information about violations to law enforcement and other competent authorities in cases provided for by law.

8. Enforcement and Sanctions

8.1. Depending on the nature of the violation, the Company may:

8.1.1. issue a warning demanding that the violation be remedied;

8.1.2. temporarily limit resources or individual functions of the service (including blocking ports and filtering traffic);

8.1.3. suspend the services;

8.1.4. terminate the service agreement without a refund of the funds paid.

8.2. In emergency cases (a threat to the network, security or third parties — DDoS attacks, phishing, malware, CSAM), measures are applied immediately, without prior notice.

8.3. Repeated or gross violations lead to permanent termination of service.

8.4. If a service is suspended due to a violation, the Client's data is retained in the manner provided for by the Terms of Service: for 2 (two) calendar days from the moment of suspension, after which it may be irretrievably deleted without any possibility of recovery.

8.5. The application of measures under this Policy does not release the Client from the obligation to compensate the Company for the losses caused.

9. Abuse Reports

9.1. Complaints about violations of this Policy shall be sent to **abuse@uphost.cloud**, specifying the time of the incident (preferably in UTC), logs and the affected IP addresses/domains.

9.2. For effective consideration, a complaint should contain:

9.2.1. a description of the violation and its nature;

9.2.2. the date and time of the incident, including the time zone;

9.2.3. the affected IP addresses, domain names and/or URLs;

9.2.4. supporting materials: logs, e-mail headers, screenshots, traffic samples;

9.2.5. the complainant's contact details for feedback.

9.3. The Company considers all reports and works with clients to remedy violations, in the following order:

9.3.1. each complaint is registered; receipt is acknowledged to the complainant, as a rule, within 1 (one) business day;

9.3.2. where indications of a violation are confirmed, the Client is sent a notice demanding that the violation be remedied, as a rule, within 24 (twenty-four) hours; in the case of critical violations (phishing, malware, attacks, CSAM), the service is suspended immediately;

9.3.3. if the violation is not remedied within the established period, the service is suspended without further notice;

9.3.4. following consideration, the Company informs the complainant of the measures taken, to the extent permissible under data protection legislation;

9.3.5. copyright infringement complaints are considered where the specific materials are identified, the complainant's rights are confirmed and a good-faith statement is provided.

9.4. Deliberately false complaints are treated as abuse and may result in the suspension of the complainant's

account and/or refusal to consider their subsequent reports.

10. Policy Changes

10.1. The Company reserves the right to amend this Policy in connection with changes in legislation, technology or the terms of service provision.

10.2. The updated version is published on the official website. Continued use of the services after the changes take effect constitutes the Client's agreement with the new version.

10.3. This Policy is governed by the laws of England and Wales.

Company Information

UPHOST SOLUTIONS LIMITED

Company number: 17188833

128 City Road, London EC1V 2NX, United Kingdom

E-mail: support@uphost.cloud

Complaints and abuse: **abuse@uphost.cloud**

Official website: https://uphost.cloud

Client area: https://my.uphost.cloud