serv.host

ACCEPTABLE USE POLICY (AUP)

SERV.HOST GROUP LTD — serv.host Services

Date of publication: 3 August 2026. Version 4.

This Policy takes effect on 3 August 2026, upon publication on the Website. It forms an integral part of the Service Agreements published on the Website (the Terms of Service of SERV.HOST GROUP LTD and the Russian Offer of the Russian partner) and applies to all Services regardless of the contracting party selected by the Customer.

1. General	1.1. This Acceptable Use Policy ("AUP") is issued by SERV.HOST GROUP LTD (Company No. 15728390, registered office: 71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ) as the operator of the serv.host platform, and defines the prohibited and restricted uses of the Services, resource and network usage rules, enforcement measures and the procedure for handling abuse reports. 1.2. The Operator reserves the right to determine, at its sole discretion, whether particular conduct constitutes a violation of this AUP, based on its own monitoring data, abuse reports and other available information. Depending on the severity of the violation, the measures provided in Section 11 may be applied after prior notice or, in the event of severe violations (Section 3), immediately and without prior notice, with subsequent notice to the Customer of the measures taken and the reasons within 24 (twenty-four) hours. 1.3. Capitalised terms used in this AUP ("Services", "Customer", "Tariff", "Account", "Ticket System", "Service Agreements") have the meanings given in the applicable Service Agreement and the User Agreement published on the Website. For contracts concluded under the Russian Offer, "Account" corresponds to the term «Учётная запись», and "Customer" is used in the meaning given in the Russian Offer. 1.4. For the purposes of this AUP, violations are classified as severe violations (Category A, Section 3) and other violations (Category B, Section 4). The Operator referred to in this AUP means SERV.HOST GROUP LTD acting as the operator of the serv.host platform; measures under this AUP are applied in respect of the Services regardless of the contracting party selected by the Customer.
2. General Principles	2.1. The Customer must use the Services responsibly, in a manner that does not degrade the performance, stability or security of the Operator's infrastructure or of the services provided to other customers. 2.2. The Customer must comply with all laws and regulations applicable to the Customer, to the hosted content and to the activity carried out through the Services, including the law of the server location, the law applicable to the relevant Service Agreement and the law of the Customer's own jurisdiction. 2.3. The Customer must take reasonable measures to protect its own servers and applications, including timely installation of security updates, strong passwords and access controls, firewalls and disabling of unused services. 2.4. The Customer must promptly notify the Operator via the Ticket System of any known compromise of its server or Account and of any security incident affecting the Services. 2.5. The Customer must hold all rights necessary for the data and software used on the Services and is solely responsible for all information, software and other materials stored on or transmitted through the Services.

	2.6. Spam, phishing and any other abusive activity are prohibited (Sections 3 and 6). 2.7. Bulk e-mail campaigns are permitted only in compliance with Section 6 of this AUP and applicable anti-spam law.
3. Severe Violations (Category A)	3.1. It is prohibited to store, publish, distribute or transmit through the Services any materials, software, data or other information that: is unlawful under applicable law; infringes copyright, related rights, patents, trademarks, trade secrets or other intellectual property rights; contains stolen, leaked or unlawfully obtained personal data, databases, accounts, access tokens, API keys, passwords, cookies, cryptographic keys or other confidential information, or materials obtained through unauthorised access or data leaks; contains malware, exploits, shellcode, webshells, remote-administration tools, command-and-control (C2) infrastructure, post-exploitation tools or other tools designed primarily for unauthorised actions, or materials intended to commit or substantially facilitate computer crimes; is used for fraud, phishing, social engineering, dissemination of deceptive information or unlawful money-making schemes (including fake login pages, scam investment schemes and counterfeit marketplaces); relates to unlawful trade in goods, services, counterfeit products or other items whose circulation is restricted or prohibited by law; promotes terrorism, extremism, violence or hatred, or contains materials of organisations banned under applicable law; contains child sexual abuse material, instructions for making prohibited items or other materials whose dissemination is prohibited by law; or violates privacy rights, contains personal data without a lawful basis or is used for harassment, blackmail, threats or other unlawful purposes. 3.2. It is prohibited to use the Services for: sending unsolicited bulk messages (spam) via e-mail, messengers, social networks, SMS or other channels; organising, carrying out or facilitating network attacks of any kind, including DoS/DDoS, flood, amplification and reflection attacks, application-layer (Layer 7) attacks, SYN flood, UDP flood and DNS amplification; unauthorised scanning of networks, ports, services and information systems; searching for, exploiting or automatically testing vulnerabilities without the consent of the owner of the relevant systems; password guessing (brute force), credential stuffing, password spraying, enumeration of verification codes and other methods of obtaining unauthorised access; spoofing of IP, ARP, DNS or MAC addresses, BGP routes or other network identifiers; exploiting open DNS, NTP, SSDP, Memcached, proxy or other services to amplify attacks or conceal their source; creating, hosting, operating or controlling botnets, C2 infrastructure, proxy networks or other means of remotely controlling malware; creating, storing, distributing or using viruses, trojans, worms, ransomware, spyware, stealers, rootkits, droppers, loaders, backdoors, cryptojackers, webshells or other malicious programs or components; carding, checking stolen payment cards or stolen credentials, circumventing anti-fraud systems or other activity connected with payment fraud; phishing, pharming, social engineering, creating fake login pages, clone websites, fraudulent online stores, investment schemes, financial pyramids or other services intended to mislead users; circumventing technical protection measures, licensing mechanisms, DRM, anti-cheat systems, authentication or other security systems; mass registration of accounts, circumventing restrictions of third-party services, artificially inflating views, followers, likes, votes, reviews, ratings or similar metrics; interfering with the operation of the platform, equipment, network infrastructure, software or the services of other customers; creating excessive load on the infrastructure or using resources in a way capable of affecting the stability or availability of the Services for other customers; or any other activity that violates applicable law, the rights and lawful interests of third parties or threatens the security of information systems. 3.3. It is also prohibited to use the Services for: operating unlicensed financial services (including payment processing, exchange and money-transfer services) and unlicensed gambling services; hosting darknet marketplaces and services intended to provide anonymous access to unlawful content; activity aimed at evading sanctions or supporting persons subject to applicable sanctions regimes; doxxing, swatting and publication of private information for the purposes of threats, harassment or intimidation; and deceptive representation of affiliation with, or endorsement by, the Operator.

	3.4. Zero tolerance: any child sexual abuse material (CSAM) results in immediate blocking of access and termination of all Services without prior notice and without refund (with subsequent notice where required by applicable law). The Operator preserves the related evidence (access logs, Account and payment data) in secure storage for at least 90 (ninety) calendar days or for such longer period as a competent authority requires, and reports the matter to the competent law-enforcement authorities. The Customer is not notified where notification could prejudice an investigation or is prohibited by law. Reports of CSAM are processed with the highest priority, outside the ordinary time limits of Section 12, and may be submitted anonymously. 3.5. Operating public (open) proxy servers, public VPN services, TOR exit nodes and other public anonymisation services without the prior written consent of the Operator is treated as a severe violation. Private VPN use for the Customer's own needs is permitted.
4. Other Violations (Category B)	4.1. The following are prohibited and are normally treated as Category B violations: storing or distributing content that infringes copyright or other intellectual property rights (including torrent seeding and file sharing of infringing materials); cryptocurrency mining, validation ("staking" using computing resources) and similar computation-farming activity, unless expressly permitted by the Tariff description or by the Operator's prior written consent, which may be made subject to resource limits and additional fees; sustained abnormal load within the meaning of Section 5; automated data collection (scraping) in breach of the terms of third-party services; deepfakes and AI-generated content infringing the rights of third parties; bandwidth-sharing and other "passive income" services; hosting pornographic content and links to it; advertising fraud, click fraud and artificial inflation of views, followers, ratings or similar metrics; operating open DNS resolvers, open SMTP relays or other misconfigured services capable of being used in amplification attacks; and keeping content that is the subject of a substantiated infringement complaint (including DMCA-type notices) after expiry of the remedy period. 4.2. In the event of a Category B violation, the Operator issues a written warning via the Ticket System or e-mail with a remedy period of no less than 24 (twenty-four) hours and no more than 5 (five) business days, unless the nature of the violation requires otherwise. If the violation is not remedied within that period, the affected Services may be restricted or suspended; repeated or unremedied violations may result in termination of the agreement in accordance with the applicable Service Agreement. 4.3. The Operator may treat a Category B violation as a severe violation (Category A) taking into account its gravity, intent, repetition and consequences. Conversely, for a first non-intentional violation (for example, where the Customer's server was compromised by third parties or misconfigured), the Operator may apply a softer measure, such as a warning or temporary restriction.
5. Resources, Traffic and IP Addresses	5.1. The Customer must stay within the resource limits of the Tariff. On plans with shared resources, sustained maximum utilisation of CPU, disk I/O or network that degrades the performance of other customers ("abnormal load") is prohibited. 5.2. For the purposes of this AUP, "sustained abnormal load" on plans with shared resources normally means utilisation of more than 90% of the allocated vCPU resources for more than 12 (twelve) hours continuously or more than 72 (seventy-two) hours cumulatively within any 7 (seven) days. Short peaks (as a rule, up to 4 (four) hours within any 24 hours) are permissible provided they do not degrade the services of other customers. 5.3. Where the stability of the infrastructure or the quality of the services of other customers is affected, the Operator may temporarily limit resources, request optimisation of the workload or offer migration to a more suitable Tariff. The Customer must reasonably cooperate with such requests. 5.4. Port bandwidth, burst speed, traffic limits and the consequences of exceeding them (including bandwidth limitation and migration

	to a Tariff with a dedicated channel and metered traffic) are governed by the applicable Service Agreement (clauses 5.11-5.14 of the Russian Offer, clauses 4.7-4.10 of the Terms of Service) and the Tariffs. Such limitations applied in accordance with the Service Agreements are not downtime under the SLA (clause 2.4 of the SLA). 5.5. It is prohibited to systematically order and cancel Services (including with refund or recalculation requests) in order to cycle through or harvest IP addresses or to circumvent blocks imposed on IP addresses. The related limit of 2 (two) recalculations per Account per calendar month is established by the Service Agreements. 5.6. IP addresses are provided for use with the Services and remain under the operator's control. Actions that result in IP addresses being blacklisted (spam databases, government registries, payment or platform blocks) are treated as a violation of this AUP; the operator may charge the actual costs of delisting or replace the affected addresses on a paid basis. 5.7. Where the Services are terminated as a result of a violation described in clause 5.6, the consequences for refunds are governed by the applicable Service Agreement and applicable law. The operator may deduct from any refundable amount its documented costs of delisting the affected IP addresses, replacing them and remedying the consequences of the violation; where such costs equal or exceed the refundable amount, no refund is made.
6. E-mail, Anti-Spam and Ports	6.1. Port 25 (SMTP) is closed by default on all Tariffs. 6.2. The Customer may request the opening of port 25 via the Ticket System. Opening is at the Operator's discretion, may require verification of the intended use and compliance with anti-spam requirements, may be made subject to an additional fee and is not guaranteed; refusal to open port 25 is not a ground for a refund. 6.3. Mass e-mail sending is permitted only in compliance with applicable anti-spam law, including prior (opt-in) consent of recipients, a working unsubscribe mechanism and accurate identification of the sender, and within the technical limits of the Tariff. The Operator may request evidence of recipients' consent and take complaint rates into account. 6.4. The Customer must maintain valid SPF, DKIM and DMARC records for domains used for sending e-mail through the Services. 6.5. The Operator may monitor aggregate sending patterns and restrict e-mail traffic where necessary to prevent abuse and maintain the reputation of its network.
7. Software Licensing	7.1. The Operator does not sell or sublicense third-party software, unless expressly stated in the Tariff or in the invoice. The "bring your own licence" model applies: the Customer independently obtains the licences it needs. 7.2. The Customer warrants that it holds valid licences for all software installed or used on the Services. 7.3. Non-activated operating-system images and installation media may be provided for convenience and testing only; the Customer is responsible for activating them with valid licence keys. 7.4. The Customer reimburses the Operator's documented losses, claims and expenses (including audit costs and penalties) arising out of the Customer's breach of software licensing terms, in accordance with the applicable Service Agreement.
8. Critical Systems	8.1. The Services are not designed for use in systems whose failure may cause harm to life, health or the environment (including medical, aviation and other safety-critical systems), or for objects of critical information infrastructure (including within the meaning of

	Russian Federal Law No. 187-FZ). The Customer confirms that it does not use the Services for such purposes; all related risks lie with the Customer.
9. Account Information Integrity	9.1. The Customer must provide accurate and complete contact information upon registration and keep it up to date in accordance with the applicable Service Agreement and the User Agreement. 9.2. Disposable or temporary e-mail addresses may not be used as the Account contact address. Privacy-oriented e-mail services with permanent mailboxes are not considered disposable. 9.3. Where the Operator reasonably suspects that the contact address is disposable or that the Account information is inaccurate, it notifies the Customer and allows no less than 48 (forty-eight) hours to update the information before applying restrictions. 9.4. Changes to contact information must be reflected in the Account within 7 (seven) calendar days. All Account information must be genuine, belong to the Customer and must not impersonate another person; for legal entities, the Account is registered by an authorised representative.
10. Security and Incident Response	10.1. Where the Customer's server is compromised or involved in abusive activity, the Operator notifies the Customer where practicable and may apply the measures provided in Section 11. 10.2. Upon the Operator's reasoned request, the Customer must promptly remediate vulnerabilities, remove malware, reinstall the operating system where necessary and change compromised credentials. 10.3. The Customer must cooperate in good faith with investigations of incidents and abuse reports and provide relevant logs and information within the limits of applicable law. 10.4. The Operator complies with binding requests of competent state, regulatory and judicial authorities of the applicable jurisdictions.
11. Enforcement	11.1. In the event of a violation of this AUP, the Operator may, taking into account the nature, duration, gravity and consequences of the violation, apply one or more of the following measures: a warning with a remedy period (no less than 24 hours and no more than 5 business days, unless the nature of the violation requires otherwise); full or partial restriction or suspension of the Services; blocking of individual resources, IP addresses, ports, network connections or traffic types; termination of the agreement in accordance with the applicable Service Agreement. In the event of severe violations (Section 3) or binding demands of competent authorities, measures may be applied immediately and without prior notice, with subsequent notice to the Customer of the measures taken and the reasons within 24 hours. 11.2. The Operator maintains an internal record of confirmed violations for each Account, reflecting their number and gravity. Repeated or systematic violations result in escalating measures, up to termination of the agreement; a single sufficiently grave violation (in particular, a Category A violation) may result in immediate termination. Complaints that are withdrawn, successfully contested or recorded in error are not counted. 11.3. The Customer must respond to abuse notifications within 24 (twenty-four) hours of the notice being sent via the Ticket System or e-mail. Failure to respond in time is an independent ground for suspension. 11.4. The Customer may submit a reasoned objection to any measure via the Ticket System, with supporting evidence. Measures

	found to have been applied in error are lifted without undue delay. 11.5. Suspension or termination of the Services due to a violation of this AUP is not compensated; the consequences for refunds are governed by the applicable Service Agreement and applicable law. The operator's system records are the primary evidence of the fact and time of a violation. 11.6. The Customer shall reimburse the operator's documented losses caused by the violation (including fines of registries and payment systems and the costs of handling abuse complaints) in accordance with the applicable Service Agreement.
12. Abuse Reports (Notice and Action)	12.1. Abuse reports are accepted at abuse@serv.host or via the Ticket System. The operator does not pre-moderate customer content and acts on the basis of received reports and its own monitoring. 12.2. A report should contain: a sufficiently substantiated explanation of why the content or activity is considered unlawful or in breach of this AUP; the exact location of the material (URL, IP address and other identifiers); the name and e-mail address of the notifier (optional for CSAM reports); and a statement that the report is submitted in good faith and that the information in it is accurate. Submission of reports is free of charge. 12.3. The Operator acknowledges receipt of a report and begins its review normally within 24 (twenty-four) hours (48 (forty-eight) hours for cases requiring in-depth analysis), reviews reports diligently and objectively, does not use solely automated decision-making for such reviews and, where contact details were provided, informs the notifier of the decision taken. 12.4. Where measures are taken against the Customer's content or Services on the basis of a report, the Customer receives a statement of the reasons and may object under clause 11.4, except where notification is prohibited by law or could prejudice an investigation (including CSAM cases under clause 3.4). 12.5. Knowingly false or malicious reports are prohibited; the Operator may refuse to process further reports from their senders. The Operator reviews all reports but is not obliged to disclose the details or results of its investigations.
13. Changes to this AUP	13.1. This AUP may be amended in the manner established by the applicable Service Agreement. The current version is published on the Website.
14. Language / Язык документа	14.1. This AUP is drawn up in English. A Russian translation is provided below for convenience; in the event of any discrepancy the English version prevails, except for relations governed by the law of the Russian Federation. 14.2. Настоящая Политика составлена на английском языке. Ниже приведён перевод на русский язык; при расхождениях преимущество имеет английская версия, за исключением отношений, регулируемых законодательством Российской Федерации.

ПОЛИТИКА ДОПУСТИМОГО ИСПОЛЬЗОВАНИЯ (AUP)

SERV.HOST GROUP LTD — услуги serv.host (перевод на русский язык)

Дата публикации: «03» августа 2026 г. Редакция № 4.

Политика вступает в силу 3 августа 2026 г. с момента публикации на Сайте, является неотъемлемой частью Сервисных соглашений, опубликованных на Сайте (Terms of Service компании SERV.HOST GROUP LTD и Публичной оферты РФ российского партнёра), и применяется ко всем Услугам независимо от выбранной Клиентом стороны договора.

1. Общие положения	1.1. Настоящая Политика допустимого использования («AUP») издана компанией SERV.HOST GROUP LTD (Company No. 15728390, зарегистрированный офис: 71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ) как оператором платформы serv.host и определяет запрещённые и ограниченные способы использования Услуг, правила использования ресурсов и сети, меры реагирования и порядок рассмотрения сообщений о нарушениях. 1.2. Оператор вправе самостоятельно определять, является ли поведение Клиента нарушением настоящей AUP, на основании результатов собственного мониторинга, поступивших жалоб (abuse-обращений) и иной доступной информации. В зависимости от тяжести нарушения меры, предусмотренные разделом 11, применяются с предварительным уведомлением Клиента либо, при грубых нарушениях (раздел 3), незамедлительно и без предварительного уведомления — с последующим уведомлением Клиента о принятых мерах и причинах их применения в течение 24 (двадцати четырёх) часов. 1.3. Термины, используемые в настоящей AUP с заглавной буквы («Услуги», «Клиент», «Тариф», «Аккаунт», «Тикет-система», «Сервисные соглашения»), имеют значения, установленные применимым Сервисным соглашением и Пользовательским соглашением, опубликованными на Сайте. Для договоров, заключённых по Публичной оферте РФ, термин «Аккаунт» соответствует термину «Учётная запись», а термин «Клиент» используется в значении Публичной оферты РФ. 1.4. Для целей настоящей AUP нарушения подразделяются на грубые нарушения (категория A, раздел 3) и иные нарушения (категория B, раздел 4). Под Оператором в настоящей AUP понимается SERV.HOST GROUP LTD как оператор платформы serv.host; меры по настоящей AUP применяются в отношении Услуг независимо от выбранной Клиентом стороны договора.
2. Общие принципы	2.1. Клиент обязан использовать Услуги ответственно — так, чтобы не ухудшать производительность, стабильность и безопасность инфраструктуры Оператора и услуг, предоставляемых другим клиентам. 2.2. Клиент обязан соблюдать все законы и нормативные акты, применимые к Клиенту, размещаемому контенту и осуществляемой через Услуги деятельности, включая право места размещения сервера, право, применимое к соответствующему Сервисному соглашению, и право юрисдикции самого Клиента. 2.3. Клиент обязан принимать разумные меры защиты собственных серверов и приложений, включая своевременную установку обновлений безопасности, надёжные пароли и контроль доступа, межсетевые экраны и отключение неиспользуемых сервисов. 2.4. Клиент обязан незамедлительно уведомлять Оператора через Тикет-систему о ставшей ему известной компрометации своего сервера или Аккаунта, а также об инцидентах безопасности, затрагивающих Услуги. 2.5. Клиент обязан обладать всеми правами, необходимыми для используемых на Услугах данных и программного обеспечения, и несёт единоличную ответственность за всю информацию, программное обеспечение и иные материалы, размещаемые на Услугах или передаваемые через них. 2.6. Спам, фишинг и любая иная злоупотребительная активность запрещены (разделы 3 и 6). 2.7. Массовые e-mail-рассылки допускаются только с соблюдением раздела 6 настоящей AUP и применимого

	законодательства о спаме и рекламе.
3. Грубые нарушения (категория А)	3.1. Запрещается хранить, публиковать, распространять, передавать или иным образом использовать посредством Услуг материалы, программное обеспечение, данные или иную информацию, которые являются незаконными по применимому законодательству; нарушают авторские, смежные, патентные, товарные знаки, коммерческую тайну либо иные права интеллектуальной собственности; содержат украденные, утёкшие либо незаконно полученные персональные данные, базы данных, учётные записи, токены доступа, API-ключи, пароли, файлы cookie, криптографические ключи либо иную конфиденциальную информацию; содержат материалы, полученные в результате несанкционированного доступа либо утечки информации; содержат вредоносное программное обеспечение, эксплойты, shell-коды, webshell, средства удалённого управления, C2-инфраструктуру, инструменты постэксплуатации либо иные средства, предназначенные преимущественно для совершения несанкционированных действий; предназначены для совершения компьютерных преступлений либо существенно облегчают их совершение; используются для мошенничества, фишинга, социальной инженерии, распространения ложной информации с целью обмана пользователей, реализации схем незаконного получения денежных средств либо иных мошеннических действий; связаны с незаконным оборотом товаров, услуг, контрафактной продукции либо иных объектов, оборот которых ограничен или запрещён законом; пропагандируют терроризм, экстремизм, насилие, разжигание ненависти либо содержат материалы организаций, деятельность которых запрещена применимым законодательством; содержат материалы сексуальной эксплуатации детей, инструкции по изготовлению запрещённых предметов или иные материалы, распространение которых запрещено законодательством; нарушают право на неприкосновенность частной жизни, содержат персональные данные без законных оснований либо используются для преследования, шантажа, угроз или иных противоправных целей в соответствии с применимым законодательством. 3.2. Запрещается использовать Услуги для массовой рассылки несогласованных сообщений (спама) по электронной почте, в мессенджерах, социальных сетях, SMS и иных каналах связи; организации, проведения или содействия сетевым атакам любого вида, включая DoS, DDoS, флуд, амплификацию, reflection-атаки, атаки уровня приложений (Layer 7), SYN flood, UDP flood, DNS amplification и иные аналогичные действия; несанкционированного сканирования сетей, портов, сервисов и информационных систем; поиска, эксплуатации либо автоматизированной проверки уязвимостей без согласия владельца соответствующих систем; подбора паролей (brute force), credential stuffing, password spraying, перебора кодов подтверждения и иных способов получения несанкционированного доступа; подмены IP-, ARP-, DNS-, MAC-адресов, BGP-маршрутов и иных сетевых идентификаторов; эксплуатации открытых DNS-, NTP-, SSDP-, Memcached-, прокси- и иных сервисов для усиления атак либо сокрытия их источника; создания, размещения, эксплуатации или управления ботнетами, C2-инфраструктурой, прокси-сетями либо иными средствами удалённого управления вредоносным программным обеспечением; создания, хранения, распространения или использования вирусов, троянов, червей, программ-вымогателей (ransomware), spyware, stealer-программ, rootkit, dropper, loader, backdoor, криптоджекеров, webshell и иных вредоносных программ или компонентов; проведения кардинга, проверки украденных банковских карт, похищенных учётных данных, обхода антифрод-систем либо иной деятельности, связанной с платёжным мошенничеством; организации фишинга, фарминга, социальной инженерии, создания поддельных страниц авторизации, сайтов-клонов, мошеннических интернет-магазинов, инвестиционных схем, финансовых пирамид и иных сервисов, направленных на введение пользователей в заблуждение; обхода технических средств защиты, механизмов лицензирования, DRM, античит-систем, средств аутентификации либо иных систем безопасности; массовой регистрации учётных записей, обхода ограничений сторонних сервисов, искусственной накрутки просмотров, подписчиков, лайков, голосований, отзывов, рейтингов и иных показателей; вмешательства в работу платформы Оператора, оборудования, сетевой инфраструктуры, программного обеспечения либо

	услуг других клиентов; создания чрезмерной нагрузки на инфраструктуру Оператора либо использования ресурсов способом, способным повлиять на стабильность или доступность Услуг для других клиентов; осуществления иной деятельности, нарушающей применимое законодательство, права и законные интересы третьих лиц либо создающей угрозу безопасности информационных систем. 3.3. Запрещается также использовать Услуги для: работы нелицензированных финансовых сервисов (включая обработку платежей, обменные сервисы и сервисы перевода денежных средств) и нелицензированных азартных сервисов; размещения даркнет-площадок и сервисов, предназначенных для анонимного доступа к незаконному контенту; деятельности, направленной на обход санкционных режимов или поддержку лиц, находящихся под применимыми санкциями; доксинга, «сваттинга» и публикации частной информации в целях угроз, преследования или запугивания; а также для создания ложного впечатления об аффилированности с Оператором или об одобрении Оператором деятельности Клиента. 3.4. Нулевая терпимость: любые материалы сексуальной эксплуатации детей (CSAM) влекут немедленную блокировку доступа и прекращение всех Услуг без предварительного уведомления и без возврата средств (с последующим уведомлением, когда это требуется применимым правом). Оператор сохраняет относящиеся к нарушению доказательства (журналы доступа, данные Аккаунта и платежей) в защищённом хранилище не менее 90 (девяноста) календарных дней либо в течение более длительного срока по требованию компетентного органа и передаёт сведения в компетентные правоохранительные органы. Клиент не уведомляется, если уведомление может помешать расследованию или запрещено законом. Сообщения о CSAM рассматриваются с наивысшим приоритетом вне обычных сроков раздела 12 и могут подаваться анонимно. 3.5. Организация публичных (открытых) прокси-серверов, публичных VPN-сервисов, выходных узлов TOR и иных публичных сервисов анонимизации без предварительного письменного согласия Оператора признаётся грубым нарушением. Использование частного VPN для собственных нужд Клиента разрешено.
4. Иные нарушения (категория B)	4.1. Запрещаются и по общему правилу относятся к нарушениям категории B: хранение и распространение контента, нарушающего авторские и иные права интеллектуальной собственности (включая раздачу торрентов и файлообмен с нарушающими материалами); майнинг криптовалют, валидация («стейкинг» с использованием вычислительных ресурсов) и аналогичная вычислительная деятельность, если она прямо не разрешена описанием Тарифа либо предварительным письменным согласием Оператора, которое может быть обусловлено лимитами ресурсов и дополнительной платой; длительная аномальная нагрузка в значении раздела 5; автоматизированный сбор данных (парсинг) с нарушением условий сторонних сервисов; дипфейки и сгенерированный ИИ контент, нарушающий права третьих лиц; сервисы «пассивного дохода» с раздачей пропускной способности и аналогичные; размещение порнографических материалов и ссылок на них; рекламное и кликовое мошенничество, искусственная накрутка просмотров, подписчиков, рейтингов и иных показателей; эксплуатация открытых DNS-резолверов, открытых SMTP-релеев и иных некорректно настроенных сервисов, пригодных для атак усиления; сохранение контента, являющегося предметом обоснованной жалобы о нарушении прав (включая уведомления типа DMCA), после истечения срока устранения. 4.2. При нарушении категории B Оператор направляет письменное предупреждение через Тикет-систему или по электронной почте с указанием срока устранения — не менее 24 (двадцати четырёх) часов и не более 5 (пяти) рабочих дней, если характер нарушения не требует иного. Если нарушение не устранено в срок, затронутые Услуги могут быть ограничены

	или приостановлены; повторные или неустранённые нарушения могут повлечь прекращение договора в порядке применимого Сервисного соглашения. 4.3. Оператор вправе квалифицировать нарушение категории B как грубое (категория A) с учётом его тяжести, умысла, повторности и последствий. И наоборот, при первом неумышленном нарушении (например, при компрометации сервера Клиента третьими лицами или ошибке конфигурации) Оператор может применить более мягкую меру — предупреждение или временное ограничение.
5. Ресурсы, трафик и IP-адреса	5.1. Клиент обязан соблюдать лимиты ресурсов Тарифа. На тарифах с разделяемыми ресурсами запрещена постоянная максимальная утилизация CPU, дисковых операций или сети, ухудшающая работу других клиентов («аномальная нагрузка»). 5.2. Для целей настоящей AUP «длительной аномальной нагрузкой» на тарифах с разделяемыми ресурсами по общему правилу признаётся использование более 90% выделенных ресурсов vCPU более 12 (двенадцати) часов непрерывно либо более 72 (семидесяти двух) часов суммарно в течение любых 7 (семи) дней. Кратковременные пики (как правило, до 4 (четырёх) часов в течение любых 24 часов) допустимы, если они не ухудшают работу услуг других клиентов. 5.3. При влиянии на стабильность инфраструктуры или качество услуг других клиентов Оператор вправе временно ограничить ресурсы, запросить оптимизацию нагрузки либо предложить переход на более подходящий Тариф. Клиент обязан разумно содействовать таким запросам. 5.4. Пропускная способность порта, burst-скорость, лимиты трафика и последствия их превышения (включая ограничение пропускной способности и перевод на Тариф с выделенным каналом и оплатой трафика) устанавливаются применимым Сервисным соглашением (пункты 5.11–5.14 Публичной оферты РФ, пункты 4.7–4.10 Terms of Service) и Тарифами. Такие ограничения, применённые в соответствии с Сервисными соглашениями, не являются Простоем по SLA (пункт 2.4 SLA). 5.5. Запрещается систематическое оформление и отмена Услуг (в том числе с требованиями возврата или перерасчёта) с целью перебора IP-адресов, получения новых IP-адресов либо обхода блокировок, наложенных на IP-адреса. Связанный лимит — не более 2 (двух) перерасчётов по Аккаунту (Учётной записи) в календарный месяц — установлен применимыми Сервисными соглашениями, опубликованными на Сайте. 5.6. IP-адреса предоставляются исключительно для использования совместно с Услугами и остаются под контролем Оператора. Действия Клиента, повлекшие включение предоставленных IP-адресов в чёрные списки (спам-базы, государственные реестры, списки блокировок платёжных систем, интернет-платформ и иных организаций), признаются нарушением настоящей AUP. В таком случае Оператор вправе взыскать с Клиента фактически понесённые расходы на исключение IP-адресов из соответствующих списков либо заменить затронутые IP-адреса на платной основе. 5.7. В случае прекращения оказания Услуг вследствие нарушения, указанного в пункте 5.6, последствия для возврата денежных средств определяются применимым Сервисным соглашением и применимым законодательством. Оператор вправе удержать из суммы, подлежащей возврату, документально подтверждённые расходы на исключение IP-адресов из списков блокировок, их замену и устранение последствий нарушения; если такие расходы равны сумме, подлежащей возврату, или превышают её, возврат не производится.
6. Электронная почта,	6.1. Порт 25 (SMTP) по умолчанию закрыт на всех Тарифах.

антиспам и порты	6.2. Клиент может запросить открытие порта 25 через Тикет-систему. Открытие осуществляется по усмотрению Оператора, может требовать проверки предполагаемого использования и соблюдения антиспам-требований, может быть обусловлено дополнительной платой и не гарантируется; отказ в открытии порта 25 не является основанием для возврата денежных средств. 6.3. Массовые e-mail-рассылки допускаются только при соблюдении применимого законодательства о спаме, включая предварительное (opt-in) согласие получателей, работающий механизм отписки и достоверную идентификацию отправителя, и в пределах технических лимитов Тарифа. Оператор вправе запросить доказательства согласия получателей и учитывать уровень жалоб. 6.4. Клиент обязан поддерживать корректные записи SPF, DKIM и DMARC для доменов, используемых для отправки почты через Услуги. 6.5. Оператор вправе отслеживать агрегированные показатели рассылок и ограничивать почтовый трафик, когда это необходимо для предотвращения злоупотреблений и защиты репутации своей сети.
7. Лицензирование программного обеспечения	7.1. Оператор не продаёт и не сублицензирует стороннее программное обеспечение, если иное прямо не указано в Тарифе или счёте. Применяется модель «bring your own licence»: Клиент самостоятельно приобретает необходимые ему лицензии. 7.2. Клиент гарантирует наличие действительных лицензий на всё программное обеспечение, установленное или используемое на Услугах. 7.3. Неактивированные образы операционных систем и установочные носители могут предоставляться исключительно для удобства и тестирования; ответственность за их активацию действительными лицензионными ключами несёт Клиент. 7.4. Клиент возмещает документально подтверждённые убытки, требования и расходы Оператора (включая расходы на аудит и штрафы), возникшие вследствие нарушения Клиентом условий лицензирования программного обеспечения, в порядке применимого Сервисного соглашения.
8. Критические системы	8.1. Услуги не предназначены для использования в составе систем, отказ или нарушение функционирования которых может повлечь угрозу жизни, здоровью людей, причинение вреда окружающей среде, значительный материальный ущерб либо иные тяжкие последствия, включая медицинские, авиационные, промышленные и иные критически важные системы. Также Услуги не предназначены для использования в объектах критической информационной инфраструктуры в случаях, предусмотренных Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Клиент подтверждает, что не использует Услуги для указанных целей, и самостоятельно несёт ответственность за последствия такого использования, если оно имело место.
9. Достоверность данных Аккаунта	9.1. Клиент обязан предоставлять точные и полные контактные данные при регистрации и поддерживать их актуальность в соответствии с применимым Сервисным соглашением и Пользовательским соглашением. 9.2. Одноразовые и временные адреса электронной почты не могут использоваться в качестве контактного адреса Аккаунта. Ориентированные на конфиденциальность почтовые сервисы с постоянными ящиками одноразовыми не считаются.

	9.3. При обоснованном подозрении, что контактный адрес является одноразовым либо данные Аккаунта недостоверны, Оператор уведомляет Клиента и предоставляет не менее 48 (сорока восьми) часов на обновление данных до применения ограничений. 9.4. Изменения контактных данных должны быть отражены в Аккаунте в течение 7 (семи) календарных дней. Все данные Аккаунта должны быть подлинными, принадлежать Клиенту и не выдавать его за другое лицо; для юридических лиц Аккаунт регистрируется уполномоченным представителем.
10. Безопасность и реагирование на инциденты	10.1. При компрометации сервера Клиента или его вовлечении в злоупотребительную активность Оператор уведомляет Клиента, когда это практически возможно, и вправе применить меры, предусмотренные разделом 11. 10.2. По мотивированному запросу Оператора Клиент обязан оперативно устранить уязвимости, удалить вредоносное программное обеспечение, при необходимости переустановить операционную систему и сменить скомпрометированные учётные данные. 10.3. Клиент обязан добросовестно содействовать расследованию инцидентов и abuse-обращений и предоставлять относящиеся к делу журналы и сведения в пределах, допускаемых применимым правом. 10.4. Оператор исполняет обязательные запросы компетентных государственных, регуляторных и судебных органов применимых юрисдикций.
11. Меры реагирования	11.1. В случае нарушения настоящей AUP Оператор вправе с учётом характера, продолжительности, тяжести и последствий нарушения применить одну или несколько мер: направление предупреждения с требованием устранить нарушение в установленный срок (не менее 24 часов и не более 5 рабочих дней, если характер нарушения не требует иного); полное или частичное ограничение либо приостановление предоставления Услуг; блокировку отдельных ресурсов, IP-адресов, портов, сетевых соединений или отдельных видов трафика; прекращение действия договора в порядке, предусмотренном применимым Сервисным соглашением. При грубых нарушениях (раздел 3) либо при наличии обязательных требований компетентных органов меры могут применяться незамедлительно и без предварительного уведомления — с последующим уведомлением Клиента о принятых мерах и причинах их применения в течение 24 часов. 11.2. Оператор ведёт внутренний учёт подтверждённых нарушений по каждому Аккаунту, отражающий их количество и тяжесть. Повторные и систематические нарушения влекут нарастающие меры вплоть до прекращения договора; одно достаточно серьёзное нарушение (в частности, нарушение категории A) может повлечь немедленное прекращение. Отозванные, успешно оспоренные или ошибочно зафиксированные жалобы не учитываются. 11.3. Клиент обязан отвечать на abuse-уведомления в течение 24 (двадцати четырёх) часов с момента направления уведомления через Тикет-систему или по электронной почте. Отсутствие ответа в срок — самостоятельное основание для приостановления. 11.4. Клиент вправе направить мотивированное возражение против применённой меры через Тикет-систему с приложением подтверждающих сведений. Меры, применённые ошибочно, отменяются без необоснованной задержки. 11.5. Приостановление или прекращение Услуг вследствие нарушения настоящей AUP не компенсируется; последствия для возвратов определяются применимым Сервисным соглашением и применимым правом. Системные записи Оператора

	являются основным доказательством факта и времени нарушения. 11.6. Клиент возмещает документально подтверждённые убытки Оператора, причинённые нарушением (включая штрафы реестров и платёжных систем и расходы на обработку abuse-жалоб), в порядке, предусмотренном применимым Сервисным соглашением.
12. Сообщения о нарушениях (notice and action)	12.1. Сообщения о нарушениях принимаются на abuse@serv.host или через Тикет-систему. Оператор не осуществляет предварительную модерацию контента клиентов и действует на основании поступивших сообщений и собственного мониторинга. 12.2. Сообщение о нарушении должно содержать: достаточно обоснованное объяснение, почему контент или деятельность считаются незаконными либо нарушающими настоящую AUP; точное расположение материала (URL, IP-адрес и иные идентификаторы); имя (наименование) и адрес электронной почты заявителя (для сообщений о CSAM — по желанию); заявление о добросовестности и достоверности изложенных сведений. Подача сообщений бесплатна. 12.3. Оператор подтверждает получение сообщения и приступает к его рассмотрению, как правило, в течение 24 (двадцати четырёх) часов (48 (сорока восьми) часов — для случаев, требующих углублённого анализа), рассматривает сообщения добросовестно и объективно, не использует исключительно автоматизированные средства для принятия решений и, если заявитель указал контактные данные, уведомляет его о принятом решении. 12.4. Если по результатам рассмотрения к контенту или Услугам Клиента применены меры, Клиенту предоставляется изложение причин, и он вправе возразить в порядке пункта 11.4, за исключением случаев, когда уведомление запрещено законом либо может помешать расследованию (включая случаи CSAM по пункту 3.4). 12.5. Заведомо ложные и недобросовестные жалобы запрещены; Оператор вправе отказать в рассмотрении дальнейших сообщений их отправителей. Оператор рассматривает все сообщения, но не обязан раскрывать детали и результаты своих расследований.
13. Изменение AUP	13.1. Настоящая AUP может изменяться в порядке, установленном применимыми Сервисными соглашениями, опубликованными на Сайте. Актуальная версия AUP публикуется на Сайте.