HOSTUP

Acceptable Use Policy

Hostup AB · Version 1.1 · 26 September 2026

This Acceptable Use Policy (the "AUP") sets out how the services of Hostup AB, reg. no. 559290-1325 ("Hostup"), may be used. It supplements the Terms of Service. A breach of this policy may lead to resources being limited or the service being suspended. It replaces version 1.0 of 1 June 2025.

---

1. How we handle breaches

1.1 If we detect a breach, we normally warn you first so that you can fix it without interruption. When there is ongoing harm, a serious security risk or a legal requirement, for example crypto mining or a server that has been compromised and is used for attacks, we may act immediately and without warning to protect the platform and others. A temporary measure of that kind does not have to wait for an investigation.

1.2 In most cases we proceed as follows:

a) **Warning or limit.** We send an email or open a ticket explaining what is wrong, what you need to do and by when. Automatic limits under section 2 apply without a warning. During a disk or CPU limit the server stays online; used-up bandwidth follows section 2.4.

b) **Deadline.** The deadline is normally 72 hours to confirm that you have seen the message and to start fixing the problem. A shorter deadline may apply when the situation requires it. If you do not reply, or the problem is not fixed, we may limit the service further or suspend it.

c) **Serious cases.** Confirmed illegal activity, intrusion, spam campaigns or anything else that threatens the platform or other networks may lead to immediate suspension.

d) **Intentional abuse.** If an individual investigation shows that a breach was intentional, for example crypto mining, false payment or identity details, or repeated abuse after a warning, we may close your entire client account under section 1.4 of the Terms of Service. Such a decision is never made automatically.

2. VPS resources

2.1 **Disk.** Disk use is free within fair use. Fair use means that, on average over the last seven days, a VPS writes at most twice its disk size per day and reads at most 50 times its disk size per day. The write allowance is always at least 500 GB per day. A VPS with a 100 GB disk may thus write 500 GB and read 5 000 GB per day on average, and a VPS with a 400 GB disk may write 800 GB per day. Many small writes load the storage more than the data volume shows. A VPS that on average writes more than its disk size per day, with more than 500 write operations per second, is therefore also above fair use. Hostup's own copies of the data within the storage system are not counted.

2.2 If a VPS goes above fair use, disk speed is limited automatically. Writing is limited to the amount per day that fair use allows and to at most 300 write operations per second. Reading is limited to about five disk sizes per day. If a VPS writes more than 5 TB in one day, or more than three times its disk size if that is more, writing is limited straight away without waiting for the weekly average. The first limit lasts 24 hours, a second within 30 days lasts four days, and after that the limit stays until the cause has been fixed and you ask us to lift it. A VPS that reads continuously at its maximum disk speed for 20 minutes, which usually means the server is short of memory, has its read speed limited in the same way. The server is never suspended for disk use but may become noticeably slower while the limit applies.

2.3 **CPU.** RAM and storage are reserved for your VPS. CPU is shared with other customers under fair use, unless the plan states dedicated CPU. Short peaks at 100% are fine. If the server runs at full load for days, CPU

may be limited to 50% of its allocated vCPUs, so that other customers are not affected. The server stays online, and the limit is lifted when the load has returned to normal.

2.4 **Bandwidth.** Each plan includes a set amount of bandwidth per billing period. When it is used up, the server is paused, unless you have an agreement where bandwidth is charged by usage, such as a VPS paid in arrears per hour and per GB. You can buy more bandwidth in the client area at any time to start the server again. We send a notice when 80% has been used; the notice is an extra service and does not change the included amount.

2.5 **DDoS protection.** Every VPS includes network-layer (L3/L4) DDoS filtering in Hostup's own network and SYN-flood protection (SYN cookies) at no extra cost. You turn the filtering on yourself in the client area. The protection covers common network-layer attacks but not large volumetric or UDP-based attacks. Protection against those requires a separate paid agreement; contact us if you need it. When an attack threatens the network or other customers, Hostup may filter, rate-limit or temporarily block traffic to the service under attack. Being attacked is not in itself a breach of this policy.

3. Email from VPS

3.1 Outgoing traffic on port 25 is blocked by default, to protect the IP reputation of other senders in the same network. Email from a VPS is therefore sent through our relay, with MailChannels as automatic backup, which filters spam and improves delivery. You may send at most 15,000 emails per month per customer, shared across all your VPS, unless we have agreed otherwise. Current usage is shown under the VPS settings in the client area, where you can also raise the limit.

3.2 If you want to send directly from your VPS, we can allow it after reviewing your account; contact us. We may withdraw the permission in case of spam, abuse or risk to the network's IP reputation. The rules on spam in section 4 apply however you send email.

3.3 We set a strong root password from the start. If you change it, the new one must also be strong. A weak password can be cracked and let the server be used for attacks on other networks.

4. Prohibited use

4.1 The services may not be used for:

a) crypto mining, staking or validation of blockchains, whatever the load. Ordinary encryption and accepting cryptocurrency as payment are allowed;

b) illegal contests, lotteries, gambling, pyramid schemes, chain letters or unsolicited bulk messages (spam), commercial or not;

c) defamation, harassment, stalking, threats or anything else that violates the rights of others, such as privacy and publicity rights;

d) publishing or distributing defamatory, obscene or unlawful material;

e) material that infringes copyright, trademarks or other intellectual property rights of others;

f) viruses, trojans, worms or other malicious code;

g) disrupting others' access to the service, for example by overloading, flooding, spam or mail bombing;

h) collecting personal data unlawfully, for example harvesting email addresses;

i) impersonating others or using someone else's identity or payment details to deceive;

j) unauthorised access, network probing or port scanning without explicit permission from the owner of the network or host;

k) offering DoS or DDoS protection as a service.

4.2 All use must comply with applicable laws and regulations.

4.3 **Addon domains.** You may add domains in cPanel as addon domains only if you own them or have written permission from the owner. Made-up domains, such as xyz.test, are not allowed. Hostup may claim damages

for a breach.

4.4 **VPN, proxy and Tor.** You may run a VPN or proxy on a VPS, for your own use or as a service for others, paid or free. If others use it, you are responsible for their traffic as for your own. You act on the abuse reports we forward to you. We may require you to block traffic that leads to repeated reports, for example BitTorrent. Public proxy servers that anyone can use without logging in, and Tor exit nodes, are not allowed. They harm the IP reputation of all customers, so that for example Google starts showing reCAPTCHA to everyone because of a single user.

5. Ordering and support

5.1 Turn off any VPN or proxy when you place your first order, so that the account can be reviewed. Once the account is approved, you may order with a VPN on.

5.2 You must give correct details, such as name and address, when ordering. When we review an order, we compare the account, payment and verification details available to us. A mismatch may lead to an extra check but is not in itself treated as fraud. If we conclude after investigation that you deliberately gave false details, for example ordering with someone else's card or identity, we close your client account and bar you from future purchases. Honest mistakes, such as a typo or a card in a family member's name, are not treated as fraud; we may then ask you to confirm your details.

5.3 Support covers Hostup's services. It does not cover administering your operating system, applications or third-party add-ons, unless that is part of what you ordered. We may limit repeated duplicate tickets, harassment of staff and unreasonable use of support. A fault in our own service is never held against you, however many tickets it causes.

5.4 We are happy to help with problems concerning our services, but not with things outside them, such as a WordPress plugin. If the developer cannot be reached, we can refer you to third-party support for a fee, which is agreed before any work starts.

6. Reporting abuse and illegal content

6.1 Report suspected illegal content or abuse to abuse@hostup.se, in Swedish or English. State where the content is (for example the exact URL), why you consider it illegal, any evidence, and your name and email address; a name and email address are not needed for a report of child sexual abuse. Confirm that the information is correct and complete to the best of your knowledge. If you have given an email address, we confirm receipt and tell you our decision, how you can contest it and whether automated tools were used. Reports may be sorted automatically, but decisions on intentional abuse are always taken by a person. A customer whose content, service or account we remove, restrict or terminate is told why and how to contest the decision. Protective measures under section 1.1 may be taken before an investigation is finished.

6.2 If you are unsure what is allowed, contact support.