Acceptable Use Policy

Last Revised: 2023-07-07

⚠ WARNING ⚠

Abuse of your service will result in your accounts being suspended or terminated. Each customer is responsible for any misuse on our systems/network.

This acceptable use policy defines Sheernox Technology Group's and its included subsidiaries and divisions policy designed to protect Sheernox Technology Group and persons and entities using Sheernox Technology Group products and services, including Internet service (collectively, "customers") from negative impact caused by inappropriate activities. Sheernox Technology Group reserves the right to modify this policy from time to time. Customers shall adhere to this policy and are subject to the terms and conditions herein.

Each customer's use of Sheernox Technology Group's products and/or services constitutes acceptance of the Acceptable Use Policy in effect at the time of use. If at any time a customer elects not to accept this policy, the customer shall discontinue use of Sheernox Technology Group's products and/or services.

Each customer is responsible for ensuring that its access to and management activities on its systems, data and content does not impose risks to or negative impacts on Sheernox Technology Group or other sites or systems.

Each customer is responsible for any misuse of accounts on its systems located at Sheernox Technology Group. Each customer shall adhere to all local, state, federal and international laws and regulations regulating customer operations.

#1 – UNACCEPTABLE USAGE

Every customer is accountable for ensuring that any systems they host with Sheernox Technology Group are not knowingly employed for the activities listed below:

1. The posting, transmission, re-transmission, or storage of material through any products or services provided by Sheernox Technology Group, if Sheernox Technology Group deems such actions to be: (a) in violation of any local, state, federal, or international law or regulation; (b) harassing (due to language, frequency, or size of message); (c) obscene; (d) hateful; or (e) libelous.
2. The installation or distribution of unlicensed or "pirated" software products.
3. The engagement in deceptive marketing practices.
4. Actions that inhibit the use or enjoyment of Sheernox Technology Group's products and services by Sheernox Technology Group or its customers, or actions that generate excessive network traffic through automated or manual routines unrelated to standard personal or business use of Internet services.
5. The introduction of malicious programs (e.g., viruses, Trojan horses, and worms) into Sheernox Technology Group's network, servers, or other products and services.
6. Any action leading to or attempting to lead to security breaches or disruptions of Internet communications. Examples include accessing data not intended for the customer or logging into a server or account without explicit authorization. Disruptions may involve port scans, flood pings, packet spoofing, and forged routing information. The use of IRC on the network is also prohibited.
7. Any form of network monitoring that intercepts data not intended for the customer.
8. Circumventing user authentication or security of any host, network, or account. This includes, but is not limited to:
    a. System configuration to bypass security controls.
    b. Conducting online security audits or tests without prior agreement and explicit written consent from a Sheernox Technology Group authorized manager.
    c. Installation of software or system configuration for "sniffing" data on a shared network.
    d. The use of software to crack encrypted data, including stored passwords.
    e. The removal or disabling of security software or services, such as anti-virus software, logging utilities, or authentication services.
9. Interference with, or denial of service to, any user other than the customer's host (e.g., denial of service attack).
10. The use of any program/script/command, or sending messages of any kind, designed to interfere with or disable a user's terminal session.

11. Providing false or incorrect data on the order form contract (whether electronic or paper), including fraudulent use of credit card numbers, or attempts to circumvent or alter the procedures to measure time, bandwidth utilization, or other methods to document the use of Sheernox Technology Group’s products or services.
12. Sending unsolicited mail messages, including "junk mail" or other advertising material to individuals who did not specifically request such material or with whom the customer does not have a pre-existing business relationship (e.g., e-mail "spam").
13. Solicitations of mail or any other e-mail address with the intent to harass or collect replies, other than that of the poster's account or service.
14. Creating or forwarding "chain letters" or other types of "pyramid schemes".
15. Using unsolicited e-mail originating from within the Sheernox Technology Group network or networks of other Internet service providers to advertise any service hosted by or connected via the Sheernox Technology Group network.
16. Exporting, re-exporting, or allowing downloads of any content in violation of the export or import laws of the United States or without all required approvals, licenses, and exemptions.
17. Engaging in high-yield investment programs.
18. Creating websites that are attacking in nature, such as "sucks" types sites, or using others' corporate names or logos to defame them.
19. Unauthorized modification of any system belonging to Sheernox Technology Group, another customer, or any other system on the Internet.
20. Violating the privacy rights of others, including unauthorized collection of personal information.
21. Participating in or permitting any activity that leads to a degradation or denial of service for Sheernox Technology Group, another customer, or any other system or site on the Internet.
22. Violating the rules or policies of any other hosting provider, message service, chat room, bulletin board, newsgroup, or similar system, service, or provider.
23. Omitting, forging, deleting, or misrepresenting transmission information intended to cloak or hide the identity or source of information transmitted by the customer’s systems or users.
24. Using the service for public IRC interconnections, such as hosting an IRC daemon or providing shell services where IRC clients and or bots are utilized.
25. Using the service primarily for email services, including free email services to the public, opt-in lists, double opt-in, or any form of regular bulk email services.
26. Hardware:
    a. Utilizing Sheernox Technology Group's services to operate server programs, including mail servers, IRC servers, game servers, FTP servers, web servers, or streaming audio/video servers.
    b. Using Sheernox Technology Group's services to sell, lease, or rent hardware or software, without a written agreement with Sheernox Technology Group.

27. Facilitating a Violation of this Policy: Providing any software, program, product, or service designed to violate this Policy, including facilitating spam, pinging, flooding, mailbombing, denial of service attacks, and software piracy.
28. Unauthorized Access: Accessing computers, accounts, or networks belonging to another party without authorization, or attempting to penetrate others' system security (often known as "hacking"). This also includes any activity that may precede an attempted system penetration, like a port scan, stealth scan, or other information gathering activity.
29. Distributing information regarding the creation and dissemination of Internet viruses, worms, Trojan horses, pinging, flooding, mailbombing, or denial of service attacks. This also includes activities that disrupt or interfere with others' effective use of the network or any connected network, system, service, or equipment.
30. Export Control Violations: Exporting encryption software over the Internet or otherwise, to points outside the United States.
31. Usenet Groups: Sheernox Technology Group reserves the right to refuse postings from newsgroups where we have knowledge that the content of the newsgroup violates the Acceptable Use Policy (AUP).
32. Other Illegal Activities: Engaging in activities determined to be illegal, including, but not limited to, advertising, transmitting, or making available Ponzi schemes, pyramid schemes, fraudulent credit card charges, and pirating software.
33. Other Activities: Engaging in activities, lawful or unlawful, that Sheernox Technology Group determines to be harmful to its subscribers, operations, reputation, goodwill, or customer relations.

Please note that the actions listed above are not exhaustive, and Sheernox Technology Group reserves the right to terminate or suspend a customer's access based on other inappropriate behavior not listed here. Sheernox Technology Group maintains a strong stance against any form of child exploitation and will cooperate fully with law enforcement in any such investigations.

#2 - PROHIBITED USES

The following uses are expressly prohibited under this Acceptable Use Policy. Engaging in any of these activities may result in immediate suspension and/or termination of your account with Sheernox Technology Group:

1. **Denial of Service (DoS) Attacks:** Engaging in activities that cause or could cause disruption to the services of others, including DoS attacks.
2. **Port Scanning:** Unauthorized scanning of open ports on any network device.
3. **Botnets:** Hosting, managing, distributing, or linking to botnets.
4. **Tor Exit Nodes:** Running Tor exit nodes on servers.

5. **Open Proxies:** The operation of open proxy servers which can be abused for various malicious activities.
6. **Open DNS Resolvers:** Running open DNS resolvers which can be used to amplify DDoS attacks.
7. **Hola:** Using or running Hola services or similar VPN anonymizing tools that may be abused for illicit activities.
8. **Unauthorized Downloads/Piracy:** Hosting, distributing, or linking to pirated or illegal content, including but not limited to software, movies, and music.
9. **Kloxo:** Utilizing Kloxo software or any software that poses significant security risks.
10. **Video Chat Services:** Hosting video chat services, including but not limited to CamFrog and Visichat, which can cause excessive server load.
11. **Cryptocurrency Mining:** Using server resources for the mining of cryptocurrencies such as Bitcoin, Ethereum, and other similar virtual currencies.
12. **HentaiAtHome:** Operating HentaiAtHome services, or any service that shares explicit content without the necessary permissions and licenses.
13. **Automated Social Media Crawlers:** Running automated data collection programs that scrape content from social media platforms such as Facebook and Twitter.
14. **IP Spoofing:** Any activities involving the falsification of network packet headers to hide, obfuscate or impersonate source IP addresses.
15. **Fraudulent Websites:** Creating or hosting websites selling or promoting fake/replica products.
16. **Phishing:** Hosting, distributing, or linking to phishing content, or any activity that attempts to unlawfully obtain sensitive information.
17. **Distributed Computing Projects:** Running distributed computing projects such as World Community Grid, Folding at Home, or similar software which can lead to excessive resource usage.
18. **Prime95:** Using Prime95 or similar stress-testing software which can lead to excessive server load.
19. **CrystalMines:** Operating CrystalMines software, or any similar program that negatively impacts server resources.
20. **Anonymization Websites:** Hosting websites designed to obfuscate or hide user IP addresses (HYIP).
21. **DDoS Services:** Hosting, distributing, or linking to DDoS-for-hire services, or any service used to amplify Denial of Service attacks (Booter/Stresser websites).
22. **Traffic Exchange Programs:** Using traffic exchange programs like HitLeap, 10KHits or any artificial traffic creation services that can lead to network congestion.
23. **Search Engine Submission Software:** Operating search engine submission software like iBusinessPromoter or similar programs that can lead to spamming.
24. **LIULIANGKUANG:** Utilizing LIULIANGKUANG or similar services that generate artificial traffic.

25. **Card Sharing Software:** Operating Multics, CCcam, or any other card sharing software that facilitates piracy.
26. **Unlicensed Game Servers:** Hosting unlicensed private game servers, particularly those targeting Chinese markets, and related websites.

Please be advised that this list is not exhaustive, and Sheernox Technology Group reserves the right to take corrective action against other forms of abusive behavior not listed here, at its sole discretion. We maintain a strong commitment to ensuring a high-quality, secure, and lawful hosting environment for all of our customers.

#3 - NO UNLAWFUL OR PROHIBITED USE

As a condition of your use of the Services, you will not use the Services (nor will you permit an end user to use the Services) for any purpose that is unlawful or otherwise prohibited by this AUP. You may not use the Services (nor will you permit an end user to use the Services) in any manner that could damage, disable, overburden, or otherwise impair any of the Services offered by Sheernox Technology Group, or any services offered by a third party, or interfere with any other party's use and enjoyment of any of our Services. You may not (nor will you permit your end users to) attempt to gain unauthorized access to any Service, other accounts, computer systems or networks connected to our network through hacking, password mining or any other means. You may not (nor will you permit your end users to) obtain or attempt to obtain any materials or information through any means not intentionally made available through the Services.

#4 – HOSTING RESOURCE USAGE POLICY

Server resources in a shared hosting environment are akin to a common pool resource; though abundant system resources are advantageous for all users, individual users often lack the motivation to moderate their usage. In order to prevent an excessive resource consumption scenario, we have established limitations on the quantity of a server's resources that a user may utilize. While these constitute defined limits, server abuse is not confined to these policies. The final determination of what constitutes server abuse resides with Sheernox Technology Group.

Please be advised that these policies are instituted for the purpose of safeguarding the quality of service provided to you, our valued customers. Typically, if a restriction needs to be imposed on an account for resource abuse, the account is likely violating at least two of these policies (or one policy to a serious extent) and is detrimentally impacting the experience of other users on the server. It is noteworthy that over 99.5% of users will likely never need to be concerned about these limitations. Nonetheless, it is beneficial to be cognizant of them. This policy aligns with our Terms of Service.

#4.1 – SHARED, RESELLER, AND RELATED HOSTING SERVICES

Services such as MySQL databases, subdomains, POP3 mail accounts, SMTP mail accounts, and FTP accounts must be utilized judiciously to prevent any potential negative impact on the optimal operation of our services. Please adhere to the following usage guidelines for Shared and Reseller accounts:

A. **MySQL databases:** Limit the number of simultaneous connections and use efficient queries to prevent excessive server load. Avoid making more than 25 simultaneous connections to a MySQL database.
B. **Subdomains:** The creation of subdomains should be limited to a reasonable number that aligns with the nature of your website. Excessive creation of subdomains can lead to resource overuse.
C. **POP3/SMTP mail accounts:** Automated sending of emails should be limited to prevent server IP blacklisting. We recommend not sending more than 500 emails per hour.
D. **FTP Accounts:** Limit the number of FTP accounts to necessary users only, and limit simultaneous connections to prevent server overloading. Avoid more than 10 simultaneous connections from a single IP.
E. **Cron jobs:** All cron jobs must be configured with a "nice" value of 15 or greater (see the Unix manpage for "nice" for more information). A cron job should not execute more frequently than once every 15 minutes.
F. **Web processes:** Web processes must not fork or spawn subprocesses. Any dynamic content should be optimized to ensure quick loading times and minimize server load.
G. **Background Programs:** Programs may not run in the background or listen on a network port. If a bot, service, or daemon is required, consider a dedicated server, as these types of programs are typically not permitted on shared web hosts.
H. **File Storage:** Shared hosting accounts are not intended for the storage of personal files or backups. Ensure the files stored on your account are directly related to your website(s).
I. **Inodes:** The number of files (inodes) on your account should not exceed 250,000. Each file hosted on your account is considered an inode.
J. **Bandwidth:** Please be aware of your account's bandwidth allowance to prevent overuse. High bandwidth usage, which affects network speed for other users, may result in temporary limitations on your account.

These policies are designed to ensure a fair and optimal environment for all shared hosting users. Please be mindful of your usage to ensure a positive hosting experience for all.

#4.2 - Virtual Private Servers and Dedicated Servers:

If Sheernox Technology Group, in good faith, believes that your resource usage (including CPU, hard drive, and network connectivity usage) has or may potentially disrupt the optimal operation

of our services, we reserve the right to request that you upgrade to a dedicated server or a higher plan. Additionally, as per our Terms of Services, your service may be rate limited or subjected to additional resource limits to prevent your service from impacting other Sheernox Technology Group customers.

#5 – UNLIMITED RESOURCE POLICY

While the term "unlimited" can be subject to various interpretations, our goal is to provide you with abundant resources, disk space and bandwidth to ensure the efficient operation of your website, regardless of its traffic. The essence of our "unlimited" policy is to free you from concerns related to data usage or consumption.

However, other considerations must be accounted for. Websites that are poorly optimized could overuse CPU, RAM, or disk I/O resources, which might affect service performance for other users on shared services. In such cases, we may suggest different hosting options, including a move to a Virtual Private Server (VPS).

"Unlimited", when referring to disk space, is defined as the provision of unmetered disk space, subject to server capacity constraints. For more information, please refer to our Terms of Services.

#5.1 - EMAIL ACCOUNTS

Although there may be no limit on the number of email accounts for unlimited email packages, each individual account **should not exceed 30GB**. This helps ensure efficient filesystem performance. Additionally, deleted emails should be cleared from the server at least annually. Further restrictions include:

A. Mailing lists must not exceed 1,500 members. Larger lists will require a semi-dedicated, VPS, or dedicated server. Dividing a large list into smaller parts to circumvent this limit is not permitted.
B. Mailing lists of over 900 emails can only be sent during off-peak times, such as weekends or between 1 am and 8 am local server time on weekdays.
C. Emails sent through a mailing list must be throttled to at least a 3-second interval between each email. This is to prevent server overloading.
D. Direct SMTP mailing system scripts are not permitted. Mail should be relayed through the local MTA.
E. Using acquired or purchased mailing lists is strictly prohibited, as it is considered spamming.

#5.2 - DATABASES

Although you may have an unlimited number of databases, unless specified by your plan, each database should be well-optimized and **should not exceed 10GB**. This is to ensure site and server performance. Usage restrictions include:

A. A maximum of 20 concurrent MySQL connections per user.
B. Database queries should not exceed 3,000 per hour, and changes (insert/update/delete) should not exceed 1,000 queries per hour.
C. Database servers must not be used as a hosting solution and should only be used for the website hosted by us.
D. Remote database access is strictly for administrative purposes.

#5.3 - RESTRICTIONS ON "UNLIMITED" USAGE

Certain uses of "unlimited" resources are not permitted to maintain fairness and quality of service. These include:

A. Hosting copyrighted material without permission from the rights holder.
B. Operating file upload/sharing/archiving/backup/mirroring/distribution sites.
C. Creating sites solely to funnel visitors to another site, also known as doorway or gateway sites.
D. Sharing your account resources with third parties, either freely or via a subscription.
E. Offering Image, File, Document and Data storage and free hosting and email services.
F. Off-site media storage is not permitted.
G. A directory cannot contain more than 2,500 immediate child files, including subdirectories but excluding files within these directories.
H. A single log file (such as a ruby production.log) should not exceed 1 GB in size, and the total size of all similar log files should not exceed 5 GB.

#6 - ENFORCEMENT

1. Each customer is obligated to enforce measures and procedures that prevent unauthorized access or usage of their systems.
2. In case of a violation, customers are expected to take immediate, reasonable and necessary action to prevent further misuse of resources.

3. Sheernox Technology Group can be alerted about policy violations through various channels, including external organizations, agencies, entities, individuals impacted by a customer's activities, or through internal detection within Sheernox Technology Group. The right to determine whether a policy violation has occurred resides solely with Sheernox Technology Group.
4. While Sheernox Technology Group generally attempts to work with the customer to rectify policy violations, it is not obligated to do so. Based on the severity of the violation or the volume or nature of received complaints, Sheernox Technology Group reserves the absolute right to terminate service immediately at its sole discretion. However, Sheernox Technology Group will strive to notify the customer prior to or at the time of such suspension. Legal remedies for any damages, costs or expenses incurred due to policy violation by or through a customer may be sought by Sheernox Technology Group.
5. If Sheernox Technology Group suspects that systems within its facilities are being used unlawfully, improperly, or for illegal activities, it will cooperate fully with civil and/or criminal enforcement authorities investigating such uses or activities. Sheernox Technology Group also commits to supporting the investigation of unacceptable uses outlined above and any other activities that, in its sole discretion, adversely impact the operation or security of Sheernox Technology Group, customers, or other systems accessible by customers or their clients or users.
6. No failure or delay in enforcing this policy constitutes a waiver of the policy or any other right or remedy. If any provision of this policy is deemed unenforceable due to a change in law, such provision will be disregarded and the remaining policy will continue in effect.

#7 - ELECTRONIC COMMUNICATIONS PRIVACY

1. Sheernox Technology Group makes no guarantee of confidentiality or privacy of any information transmitted through or stored upon Sheernox Technology Group technology, and makes no guarantee that any other entity or group of users will be included or excluded from Sheernox Technology Group’s network. Sheernox Technology Group may periodically monitor transmissions over its network for maintenance, service quality assurance or any other purpose permitted by the Electronic Communications Privacy Act, P.L. No. 99-508, as amended.

2. GOVERNMENT SURVEILLANCE WARNING: Note that due to provisions in both the Patriot Act and the Foreign Intelligence Surveillance Act (FISA), US companies must hand over user’s data even if that user is a non-US citizen, and the data has never been stored in the US. **Sheernox Technology Group offers no protection against government surveillance programs**. Accordingly, there can be no expectation of privacy in the course of your use of any of Sheernox Technology Group’s computer systems. The use of a password or any other

security measure does not establish an expectation of privacy. There is no expectation of privacy in any form of access to Sheernox Technology Group's computer systems.

3. Warrant Canary: As of 2023-07-07 no warrants have ever been served to Sheernox Technology Group or its employees. No searches or seizures of any kind have ever been performed on Sheernox Technology Group assets. Sheernox Technology Group has no direct or indirect knowledge of any backdoors, or potential backdoors in our servers or network and Sheernox Technology Group has not received any requests to implement a backdoor. Sheernox Technology Group has never disclosed any user communications to any third party.

    - Special note should be taken if these messages ever cease being updated, or are removed from this page. However, this scheme is not infallible. This statement does not prevent them from using force to coerce Sheernox Technology Group to produce false declarations.

#8 – REPORTING VIOLATIONS

If you become aware of any violation of this AUP, you will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. To report any violation of this AUP, please contact us at **abuse@sheernox.com**