NETWORK & CLOUD INFRASTRUCTURE POLICY

Acceptable Use Policy (AUP)

Last Revised: **2026-09-12** v4.0-AUP

⚠ **CRITICAL POLICY WARNING**

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

0.0 Preamble & Scope of Customer Responsibility

IN PLAIN ENGLISH

This Acceptable Use Policy (AUP) protects Sheernox, our servers, and all clients from negative impacts caused by inappropriate activities. Sheernox Technology Group is a Canadian sole proprietorship registered at 1-1885 Grasslands Blvd, Kamloops, BC, V2B 0B8, Canada. Your use of our services constitutes continuous acceptance of this policy under British Columbia and Canadian law.

This Acceptable Use Policy defines the policy of **Sheernox Technology Group**, a sole proprietorship registered at 1-1885 Grasslands Blvd, Kamloops, BC, V2B 0B8, Canada, and its included networks, infrastructure, and operating divisions (collectively, "Sheernox"), designed to protect Sheernox and persons and entities using Sheernox products and services, including Internet service, cloud hypervisors, server hardware, and software systems (collectively, "Customers"), from negative impact caused by inappropriate or unlawful 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 immediately.

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, provincial, federal, and applicable international laws regulating customer operations.

1.0 General System & Content Standards (Illustrative Examples)

IN PLAIN ENGLISH

The rules below illustrate prohibited behavior and are not an exhaustive list. You cannot use Sheernox web hosting or VPS infrastructure for illegal activities, software piracy, network disruption, credential cracking, spam, pyramid schemes, or child exploitation. CSAM is reported immediately to Cybertip.ca and the RCMP.

Every Customer is directly accountable for ensuring that any account, website, web application, container, database, or virtual machine hosted with Sheernox Technology Group is not knowingly, recklessly, or negligently utilized for unacceptable activities. **The following provisions provide illustrative examples of prohibited conduct and do not constitute an exhaustive or exclusive list.** Sheernox reserves the absolute operational discretion to determine whether any specific conduct violates the spirit of this Policy:

- 1.1 **Unlawful, Obscene, or Defamatory Material:** The posting, transmission, re-transmission, caching, or storage of material through any products or services provided by Sheernox that: (a) violates any local, provincial, federal, or applicable

international law or regulation; (b) is legally defamatory, libelous, or scandalous; (c) constitutes hate speech or incitement to violence contrary to the *Criminal Code of Canada*; or (d) is harassing due to language, frequency, or transmission volume.

- 1.2 **Zero-Tolerance for Child Sexual Abuse Material (CSAM):** Any creation, hosting, caching, distribution, transmission, or linking to Child Sexual Abuse Material. Sheernox enforces an absolute zero-tolerance policy. Violations result in immediate permanent account termination, IP isolation, and mandatory reporting with digital evidence preservation to **Cybertip.ca** and the **Royal Canadian Mounted Police (RCMP)**.
- 1.3 **Intellectual Property Infringement & Software Piracy:** The installation, distribution, mirroring, linking to, or indexing of unlicensed software ("warez"), software cracking utilities, serial number generators, copyright-infringing digital media, or counterfeit designer goods. Infringements are addressed pursuant to the Canadian *Copyright Act* Notice-and-Notice regime.
- 1.4 **Deceptive Marketing & Consumer Fraud:** Engaging in fraudulent business practices, deceptive telemarketing, or false representations contrary to the Canadian *Competition Act* or provincial consumer protection legislation, including fake e-commerce shops, fraudulent tech support scams, and deceptive lead generation.
- 1.5 **Network & Infrastructure Degradation:** Any actions that degrade, disrupt, or impair the stability, performance, or enjoyment of Sheernox's cloud hypervisors, network transit, edge routing, or shared servers by other subscribers, or generating abnormal traffic loads unrelated to standard commercial web operations.
- 1.6 **Malicious Code & Weaponized Payloads:** Introducing, hosting, distributing, or executing malicious programs—including computer viruses, Trojan horses, ransomware, rootkits, keyloggers, worm propagation routines, or exploit kits—on or through Sheernox servers, hypervisors, or client accounts.
- 1.7 **Unauthorized Access & Intrusion Attempts:** Any action attempting to compromise, probe, or breach the security of any system, network, account, or hypervisor. This includes unauthorized access to data, attempting to bypass user authentication barriers, cracking hashed credentials, or unauthorized modification of system files.
- 1.8 **Interception & Unauthorized Monitoring:** Any form of unauthorized packet sniffing, network tapping, traffic inspection, or data interception on shared hypervisor bridges, virtual switches, or public network interfaces.
- 1.9 **Denial of Service Attacks:** Launching, participating in, facilitating, or amplifying Denial of Service (DoS or DDoS) attacks against any host, server, router, network service, or terminal session.
- 1.10 **Account & Payment Fraud:** Providing false, fictitious, or forged information on electronic account registrations, utilizing unauthorized or stolen credit cards or payment credentials, or attempting to circumvent bandwidth, disk quota, or compute metering systems.
- 1.11 **Spam & Unsolicited Communications (CASL Compliance):** Transmitting Unsolicited Commercial Electronic Messages (CEMs), bulk unsolicited emails ("spam"), or unverified marketing blasts in violation of *Canada's Anti-Spam Legislation* (CASL) and international anti-spam statutes. This includes using scraped, harvested, or purchased recipient lists, or utilizing email addresses obtained without verifiable express or implied consent.
- 1.12 **Email Forgery & Routing Manipulation:** Forging, altering, or obfuscating email transmission headers, return path addresses, DKIM signatures, or IP routing data to disguise the origin of commercial electronic messages.
- 1.13 **Ponzi, Pyramid & Fraudulent Financial Schemes:** Operating, marketing, or facilitating pyramid schemes, Ponzi schemes, fraudulent multi-level marketing (MLM), fake cryptocurrency investment platforms, or High-Yield Investment Programs (HYIP).
- 1.14 **Spam-Advertising Hosted Sites ("Spamvertising"):** Utilizing unsolicited emails or automated comment spam originating from external networks to advertise or drive traffic to any website, domain, or service hosted on Sheernox infrastructure.
- 1.15 **Export Controls & Sanctions Violations:** Exporting, re-exporting, or providing digital assets in contravention of Canadian export controls, economic sanctions, or the *Export and Import Permits Act* (R.S.C., 1985, c. E-19), including restricted cryptographic algorithms or restricted defense technology.
- 1.16 **Defamatory & Harassment Platforms:** Operating websites or services whose primary purpose is targeted harassment, doxxing, defamation, or extortion of individuals or commercial entities.
- 1.17 **Unpatched Software & Negligent Hosting:** Operating abandoned, end-of-life, or critically unpatched web software, outdated CMS installations (e.g. WordPress, Joomla, Drupal), or vulnerable web plugins that present an active security liability to shared hypervisor nodes.
- 1.18 **Privacy & Identity Violations:** Collecting, harvesting, or publishing personally identifiable information or financial credentials without statutory authorization, contrary to the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA) and British Columbia's *Personal Information Protection Act* (PIPA).

- 1.19 **Reputational & Operational Harm:** Engaging in any conduct, whether lawful or unlawful, that Sheernox determines in its professional engineering judgment to be harmful to system stability, IP reputation, upstream carrier agreements, or customer goodwill.

Please note that the examples set forth above are strictly illustrative. Sheernox reserves the full right to suspend or terminate services for any behavior, content, or system operation that compromises network integrity, security, or statutory legal compliance.

2.0 Prohibited Network & Technical Activities

> **IN PLAIN ENGLISH**
>
> Engaging in abusive network activities—such as DDoS attacks, port scanning, botnets, crypto-mining, open proxies, Tor exit nodes, or hypervisor stress-testing—results in immediate suspension or termination. These examples illustrate prohibited technical uses and are not exhaustive.

The following technical uses, background daemons, and network configurations are strictly prohibited across Sheernox shared hosting, managed servers, and Virtual Private Server (VPS) infrastructure. **The categories below provide representative technical examples and do not constitute an exhaustive catalog of prohibited actions:**

- 2.1 **Denial of Service (DoS / DDoS) Operations:** Launching, amplifying, participating in, or maintaining software designed to execute distributed denial of service attacks, SYN floods, UDP amplification, or layer-7 HTTP floods against any target.
- 2.2 **DDoS-for-Hire & Booter Platforms:** Operating, marketing, or hosting "Booter", "Stresser", IP stress-testing, or commercial DDoS-for-hire attack services and target APIs.
- 2.3 **Unauthorized Port Scanning & Network Probing:** Executing automated port scans, vulnerability probes, SYN sweeps, or unauthorized security audits against external Internet hosts or internal Sheernox IP ranges without advance written consent.
- 2.4 **Botnet Command & Control (C2) Infrastructure:** Hosting, controlling, distributing, or maintaining Command and Control (C2) servers, botnet distribution nodes, or zombie networks.
- 2.5 **Cryptocurrency Mining:** Utilizing shared hosting CPUs, VPS hypervisor cores, graphics processing units (GPUs), or NVMe storage I/O for the mining of cryptocurrencies (such as Bitcoin, Monero, Ethereum, or Chia proof-of-space plotting) without an explicit dedicated compute enterprise contract.
- 2.6 **Tor Exit Nodes & Public Darknet Relays:** Operating Tor exit nodes, I2P public gateways, or routing unverified darknet exit traffic through Sheernox IP space, which attracts blacklists and abuse complaints.
- 2.7 **Open Proxies & Unauthenticated Tunnels:** Operating open, unauthenticated HTTP, HTTPS, or SOCKS proxies, or public VPN gateways that enable third parties to route unauthorized, anonymous traffic through our network.
- 2.8 **Open Recursive DNS Resolvers:** Running publicly accessible recursive DNS resolvers that can be weaponized for UDP amplification reflection attacks.
- 2.9 **IP Spoofing & Layer-2 Manipulation:** Falsifying IP packet header source addresses, forging ARP replies, or spoofing MAC addresses across virtual network adapters.
- 2.10 **Phishing & Financial Deception Engines:** Deploying deceptive credential harvesting websites, fake banking portals, spoofed webmail authentication forms, or social engineering landing pages.
- 2.11 **Automated Traffic Generators & Hit Inflation:** Utilizing artificial traffic fabrication software, auto-surf exchanges (e.g., HitLeap, 10KHits), click-fraud bots, or automated search engine query flooding routines.
- 2.12 **Aggressive Scrapers & Form-Spam Daemons:** Running continuous automated scrapers that aggressively harvest content contrary to remote site robots.txt guidelines or terms of service, or executing automated form-spamming software.
- 2.13 **Hypervisor & Hardware Stress-Testing:** Executing synthetic benchmark stress-tests (e.g., Prime95, FurMark) or distributed compute packages (e.g., Folding@home, BOINC) that artificially pin hypervisor CPU cores or exhaust thermal envelopes to the detriment of co-hosted virtual machines.
- 2.14 **Noisy Neighbor Hypervisor Abuse:** Configuring virtual machines in a manner that monopolizes host bus adapters (HBAs), generates sustained I/O queue bottlenecks, or thrashes shared storage arrays, degrading adjacent tenant VPS performance.
- 2.15 **Unsecured Management Interfaces:** Exposing unauthenticated, sensitive control daemons directly to the public Internet, including unsecured Docker sockets, exposed Kubernetes APIs, or unauthenticated Redis, Elasticsearch, or

MongoDB database ports.

- **Media Stream Ripping & Copyright Circumvention:** Hosting automated stream-ripping software, IPTV restreaming servers, satellite card-sharing daemons (e.g., CCcam, Multics), or software designed to strip digital rights management (DRM) protections.
- **Unlicensed Private Game Emulators:** Operating unauthorized, unlicensed private server emulators for commercial games that violate intellectual property rights or frequently attract volumetric DDoS extortion attacks.

3.0 No Unlawful or Prohibited Use

3.1 Fundamental Condition: As an express condition of your use of the Services, you will not use the Services (nor permit any end-user to use the Services) for any purpose that is unlawful under Canadian law, British Columbia provincial law, or prohibited by this AUP. You may not use the Services in any manner that could damage, disable, overburden, or impair any Sheernox facility, hypervisor, router, or edge network, or interfere with any other party's use and enjoyment of the Services.

3.2 Unauthorized Access Prohibited: You may not attempt to gain unauthorized access to any accounts, computer systems, hypervisors, or networks connected to Sheernox through hacking, password mining, API exploitation, or any other unauthorized means.

4.0 Hosting & Infrastructure Resource Fair Use Policy

> **IN PLAIN ENGLISH**
>
> Shared hosting and multi-tenant VPS nodes operate on fair resource sharing. We enforce defined compute, database query, memory, and networking limits so that no single customer degrades performance for other businesses hosted on the same physical infrastructure.

Server resources in a shared hosting or multi-tenant cloud environment are communal resources. In order to ensure enterprise-grade stability, uptime, and performance for all subscribers, Sheernox enforces clear resource consumption guidelines. While numerical thresholds are established below, resource abuse is evaluated holistically; the final determination of what constitutes service degradation or unmanaged compute abuse resides exclusively with Sheernox Technology Group.

These policies safeguard the performance and quality of service provided across our network. Adherence ensures your infrastructure remains reliable, performant, and protected.

Shared, Reseller, and Managed Hosting Constraints

4.1 MySQL / MariaDB Databases:

a. Limit simultaneous database connections to reasonable levels; do not maintain permanent persistent connections that exhaust connection pools.

b. Queries executing longer than thirty (30) seconds or requiring temporary on-disk tables exceeding 2GB may be killed automatically to prevent hypervisor I/O lockup.

c. Database storage must be directly utilized by an active website hosted on the same Sheernox account. Remote database hosting for external applications is prohibited on shared plans.

4.2 Cron Job Scheduling: Automated cron jobs must not be scheduled at intervals shorter than fifteen (15) minutes. Scripts triggered by cron jobs must execute efficiently and terminate within 180 seconds. Cascading or overlapping scheduled tasks are strictly prohibited.

4.3 CPU & Memory Quotas: An account on Shared or Reseller hosting may not consume more than 25% of server CPU or 1024MB RAM continuously for longer than ninety (90) seconds. Sustained spikes will result in temporary process throttling (via CloudLinux LVE or cgroups) or a requirement to upgrade to an isolated Cloud VPS tier.

4.4 Web & Script Processes: Long-running standalone background daemons (such as shoutcast servers, background bots, or persistent websockets) may not be executed on standard shared hosting environments.

Virtual Private Servers (VPS) and Dedicated Infrastructure

IN PLAIN ENGLISH

VPS customers have administrative root access and are solely responsible for securing their operating system and applications. In the event of compromise or outbound network attacks, Sheernox may immediately isolate or null-route the server to safeguard the host hypervisor.

4.5 **Root Access & Administrative Responsibility:** Customers provisioned with root or administrative access to VPS or dedicated hardware are fully responsible for the security posture of their guest operating system, application stack, firewall configuration, user authentication, and prompt installation of vendor security patches.

4.6 **Multi-Tenant Hypervisor Fair Use & Noisy Neighbor Mitigation:** Cloud VPS instances share underlying physical host CPUs, NVMe storage fabrics, and network interfaces. Operating workloads that generate sustained 100% CPU lock, continuous memory ballooning, or excessive disk I/O thrashing that degrades adjacent tenant instances is prohibited. Sheernox may temporarily throttle or deprioritize abusive guest processes.

4.7 **Outbound Abuse, Null-Routing & Emergency Quarantine:** In the event an unmanaged VPS is compromised, generates outbound DDoS traffic, emits spam, participates in brute-force scanning, or is targeted by incoming volumetric attacks exceeding mitigation capacity, Sheernox reserves the right to immediately null-route the IP address or isolate the virtual machine on a quarantine network without prior notice to protect infrastructure integrity.

4.8 **Network Configurations & Authorized IP Addressing:** VPS customers must configure only the specific IP addresses and subnets explicitly assigned to their instance by Sheernox. Configuring unassigned IP addresses, ARP spoofing, broadcast storm generation, unauthorized DHCP servers, or bridging foreign network interfaces is grounds for immediate termination.

4.9 **Unmanaged Backup & Snapshot Responsibilities:** Unless Customer maintains an active subscription to Sheernox Managed Backup Services, Customer is solely responsible for generating, verifying, and maintaining off-site backups of virtual disk snapshots, database dumps, and application configurations.

5.0 Unlimited Resource Policy & Practical Limits

IN PLAIN ENGLISH

"Unlimited" hosting plans provide ample storage and bandwidth for typical small-to-medium business websites. They cannot be converted into free cloud backup storage, file vaults, video streaming mirrors, or mass mailing lists.

5.1 **Email Accounts:** Individual POP3/IMAP mailboxes must be utilized for normal business correspondence. Storing multi-gigabyte personal desktop file archives within email accounts is prohibited. Outbound mailing is capped at 500 emails per hour per domain on shared infrastructure.

5.2 **Databases:** Relational MySQL/MariaDB databases must support active web applications hosted directly on Sheernox infrastructure. External remote database hosting, public data repositories, or continuous IoT telemetry ingestion is not permitted under shared unlimited plans.

5.3 **Restrictions on "Unlimited" Usage:** Unlimited storage and bandwidth allotments are granted exclusively for standard website content, HTML files, stylesheets, images, and documents directly linked from the hosted domain. Accounts may not be repurposed for:

a. Off-site backup vaults, personal computer backups, or secondary disk mirrors.

b. Public file sharing repositories, ISO download mirrors, or video streaming sites.

c. Hosting torrent tracker files or file-locker distribution scripts.

6.0 Enforcement, Suspension & Blacklisting Fees

6.1 **Right to Enforce:** Failure to adhere to any provision of this AUP may result in immediate warning, temporary resource throttling, suspension, or permanent termination of service without refund.

6.2 Delisting Remediation Fee ($150 CAD): If customer activity causes Sheernox IP ranges to be blacklisted on major security registries (Spamhaus, Barracuda, SORBS, etc.), a clean-up and delisting fee of $250.00 CAD will be charged to the customer's account to cover engineering overhead.

7.0 Electronic Communications Privacy Under Canadian Law

7.1 Privacy Protections: Sheernox treats customer data and communications as confidential in accordance with the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA) and British Columbia's *Personal Information Protection Act* (PIPA).

7.2 Lawful Interception: Sheernox will not monitor, intercept, or disclose private customer communications except: (a) as required by lawful court order, search warrant, or statutory subpoena issued by a court of competent jurisdiction in Canada; (b) as necessary to protect the integrity, security, and operation of Sheernox systems; or (c) to report child exploitation material to Cybertip.ca and law enforcement.

8.0 Reporting Violations & Abuse Routing

IN PLAIN ENGLISH

To report network abuse, spam, or security violations originating from Sheernox IP allocations, submit an incident report with full log evidence to our Abuse Department.

8.1 Abuse Contact: Reports of violations of this Acceptable Use Policy originating from Sheernox IP space should be directed with full technical evidence to:

Abuse Department
Sheernox Technology Group
1-1885 Grasslands Blvd, Kamloops, BC, V2B 0B8, Canada
Email: abuse@sheernox.com
Client Portal: https://my.sheernox.com