

ACCEPTABLE USE POLICY (AUP)

Effective Date: October 19, 2025

Last Updated: August.10.2026

1. PURPOSE AND LEGAL EFFECT

This Acceptable Use Policy ("**Policy**" or "**AUP**") establishes the mandatory rules governing the access to and use of all services, infrastructure, software, platforms, systems, applications, and technology solutions provided by **RootHosts** ("**RootHosts**," "**we**," "**our**," or "**us**").

This Policy forms an integral and legally binding component of the RootHosts **Terms of Service** and shall be incorporated therein by reference. Compliance with this Policy constitutes a fundamental condition of the Customer's right to access and continue using the Services.

The primary objectives of this Policy are to:

- preserve the confidentiality, integrity, availability, and resilience of the RootHosts Infrastructure;
- safeguard the security and stability of all hosted environments;
- protect Customers, business partners, infrastructure providers, and third parties from unlawful or harmful activities;
- ensure compliance with applicable laws, regulations, industry standards, and contractual obligations; and
- maintain a secure, reliable, and professionally managed technology environment for all users.

Any use of the Services inconsistent with this Policy shall constitute a material breach of the contractual relationship between the Customer and RootHosts.

2. APPLICATION OF THIS POLICY

This Policy applies to every individual, legal entity, reseller, organization, contractor, affiliate, employee, representative, or other person accessing or using any RootHosts Service, whether directly or indirectly.

Without limitation, this Policy governs the use of:

- Shared Hosting Services;
- Dedicated Server Solutions;
- Virtual Private Server (VPS) Services;
- Cloud Infrastructure Services;
- Managed VPS Services;
- Linux and Windows Server Administration;
- System Administration Services;
- Managed Proxmox VE Infrastructure;
- Network Security Services;
- DDoS Protection Services;
- VPN Services;
- Backup and Disaster Recovery Services;
- Infrastructure Monitoring;
- Technical Consulting Services; and
- any present or future technology products, software, platforms, or managed services offered under the RootHosts brand.

3. CUSTOMER RESPONSIBILITIES

The Customer shall use the Services in a lawful, responsible, ethical, and professional manner at all times.

Without limitation, each Customer shall:

- comply with all applicable local, national, European Union, and international laws;
- comply with all contractual obligations governing the Services;
- ensure that all activities performed through the Services remain lawful and properly authorized;
- implement reasonable administrative, organizational, and technical security measures;
- maintain the confidentiality of authentication credentials;
- promptly report any suspected compromise, abuse, or security incident affecting the Services.

The Customer accepts full legal responsibility for all activities conducted through its account, systems, virtual environments, users, agents, contractors, or authorized representatives.

4. PROHIBITED USE

The Services shall not be used for any activity that is unlawful, fraudulent, malicious, deceptive, harmful, abusive, negligent, or otherwise inconsistent with the intended purpose of the RootHosts Infrastructure.

Prohibited activities include, without limitation:

4.1 Illegal Conduct

Customers shall not use the Services to:

- violate any applicable law or regulation;
- facilitate criminal conduct;
- evade legal obligations;
- support illegal organizations or unlawful enterprises;
- engage in activities prohibited by governmental authorities.

4.2 Unauthorized Access

Customers shall not:

- obtain or attempt to obtain unauthorized access to any system, network, application, service, database, or account;
- circumvent authentication or security mechanisms;
- exploit vulnerabilities without authorization;
- intercept communications unlawfully;
- engage in privilege escalation;
- perform credential harvesting or password attacks.

4.3 Cybersecurity Threats

The Services shall not be used to create, distribute, deploy, execute, store, facilitate, or control:

- malicious software;
- ransomware;
- spyware;
- trojans;
- worms;
- viruses;
- botnets;
- cryptojacking software;
- exploit frameworks;
- malicious automation tools;
- remote access malware;
- command-and-control infrastructure;
- any software intended to compromise information systems.

4.4 Network Abuse

Customers shall not engage in activities including:

- Distributed Denial-of-Service (DDoS) attacks;
- Denial-of-Service (DoS) attacks;
- packet flooding;
- protocol manipulation;
- IP spoofing;
- DNS amplification;
- brute-force attacks;
- excessive vulnerability scanning;
- unauthorized penetration testing;
- routing manipulation;
- ARP poisoning;
- network interception;
- bandwidth abuse.

4.5 Fraudulent Activities

The Services shall not be used in connection with:

- phishing;
- identity theft;
- payment fraud;
- investment fraud;
- impersonation;
- account compromise;
- social engineering;
- financial scams;
- cryptocurrency fraud;
- deceptive commercial practices.

4.6 Spam and Unsolicited Communications

Customers shall not transmit or facilitate:

- unsolicited commercial email;
- bulk messaging without lawful consent;
- email header forgery;
- spam campaigns;
- open mail relays;
- unsolicited SMS campaigns;
- phishing communications;
- deceptive electronic communications.

5. CONTENT STANDARDS

Customers shall not upload, publish, distribute, transmit, process, or store any content that:

- violates applicable law;
- infringes intellectual property rights;
- violates privacy or data protection rights;
- constitutes fraud or deception;
- promotes terrorism or organized crime;
- facilitates cybercrime;
- contains malicious code;

- incites violence or hatred;
- violates court orders or governmental restrictions.

RootHosts reserves the sole discretion to determine whether hosted content presents an unacceptable legal, operational, or security risk.

6. FAIR USE OF INFRASTRUCTURE

Customers shall utilize Infrastructure resources fairly and responsibly.

Activities resulting in unreasonable or excessive consumption of computing resources, processor capacity, memory, storage, network bandwidth, virtualization resources, or shared infrastructure may adversely affect other Customers and are strictly prohibited.

RootHosts reserves the unrestricted right to implement technical limitations, isolate workloads, throttle resource consumption, suspend workloads, or otherwise protect the operational stability of its Infrastructure.

7. SECURITY REQUIREMENTS

Customers shall maintain security measures consistent with recognized industry standards, including:

- secure authentication practices;
- strong password policies;
- multi-factor authentication where available;
- timely installation of security updates;
- continuous monitoring of hosted systems;
- appropriate firewall configurations;
- secure remote administration;
- regular vulnerability remediation.

Failure to implement reasonable security controls may constitute a material breach of this Policy.

8. INVESTIGATION AND ENFORCEMENT

RootHosts reserves the unrestricted right, at its sole and reasonable discretion, to investigate any suspected violation of this Policy.

Where RootHosts reasonably determines that a violation has occurred or is likely to occur, RootHosts may immediately, and without prior notice where circumstances reasonably require, take any action deemed necessary, including:

- restricting account access;
- suspending Services;
- isolating virtual environments;
- removing hosted content;
- blocking network traffic;
- preserving electronic evidence;
- reporting unlawful conduct to competent authorities;
- terminating the contractual relationship; and
- pursuing all contractual, civil, administrative, or criminal remedies available under applicable law.

The exercise of any enforcement measure under this Policy shall not limit any additional legal rights or remedies available to RootHosts.

9. CUSTOMER INDEMNIFICATION

The Customer shall defend, indemnify, and hold harmless RootHosts, its owners, affiliates, contractors, employees, licensors, infrastructure providers, successors, and assigns from and against any and all claims, liabilities, damages, losses, penalties, regulatory actions, judgments, costs, expenses, and reasonable legal fees arising directly or indirectly from:

- any violation of this Policy;
- unlawful use of the Services;
- Customer Content;
- infringement of third-party rights;
- negligent, fraudulent, or intentional misconduct;
- any act or omission attributable to the Customer or persons acting under the Customer's authority.

10. POLICY AMENDMENTS

RootHosts reserves the absolute right to modify, supplement, replace, or update this Policy at any time where reasonably necessary to reflect legal developments, regulatory

requirements, technological advancements, operational changes, evolving cybersecurity threats, or business requirements.

The continued use of the Services following publication of the revised Policy shall constitute acceptance of the amended Policy.

11. GOVERNING LAW

This Policy shall be governed by, interpreted, and enforced in accordance with the applicable laws of the European Union together with the mandatory laws of the jurisdiction in which RootHosts lawfully operates.

12. CONTACT INFORMATION

RootHosts

Website: RootHosts.com

Billing Support: info@roothosts.com

General Support: support@roothosts.com

Legal Department: info@roothosts.com