TRANSLATION NOTICE

This document has been automatically translated from Polish to English using artificial intelligence for informational purposes only.

In the event of any discrepancies, inconsistencies, or conflicts between the English and Polish language versions of this document, **the Polish language version shall prevail and constitute the sole legally binding version**.

For official and legally binding information, users are advised to consult the original Polish language document.

Users who do not understand Polish are advised to seek independent legal advice before accepting these terms.

FAIR USE POLICY (FUP)

For the platform/website/service/services located at the domain address " voxihost.pl"

This document is part of a set of documents:

a. Terms of Service (TOS)
b. Privacy Policy (PP)
c. Service Level Agreement (SLA)
d. Fair Use Policy (FUP)

Effective Date: 14.02.2026
Last Updated: 15.01.2026

§ 1. INTRODUCTORY PROVISIONS AND DEFINITIONS

1.1. Operator:

a. VoxiHost DANIEL MARSZAŁKOWSKI
b. ul. 3 Maja 29, 62-500 Konin, Poland
c. **NIP:** 6653080651 | REGON: 542936383
d. **E-mail:** support@voxihost.pl

(hereinafter referred to as "VoxiHost" or the "Operator").

1.2. Scope of Application: This Fair Use Policy constitutes an integral part of the Terms of Service and applies exclusively within the framework of the website available under the VoxiHost.pl domain. This document does not apply to other services, projects, or websites operated by the Operator under different addresses.

1.3. Integrity: This Fair Use Policy constitutes an integral part of the set of documents listed in the header of this document.

1.4. Purpose: The purpose of the Fair Use Policy is to ensure the stability, security, and high

performance of the infrastructure for all Clients and to protect the Operator's network reputation.

1.5. Acceptance: Account registration or ordering a Service is equivalent to full acceptance of this document and all related documents. In the event of changes to the FUP, the Client will be informed in accordance with §8.1. Failure to object within 30 days of notification constitutes acceptance of the changes. The Client has the right to terminate the agreement in case of non-acceptance of the changes.

1.6. Sole Discretion with Right of Appeal: The Operator reserves the right to technical and legal assessment of whether a given action by the Client constitutes a violation of this Policy. In the event of a decision to block or impose restrictions, the Client has the right to appeal the decision within 7 days via a submission in the Support system (ticket). The appeal will be considered by an independent member of the technical team within 7 business days. The decision resulting from the appeal is final.

§ 2. NETWORK AND INFRASTRUCTURE SECURITY (NETWORK ABUSE)

Any actions that may disrupt the functioning of the Operator's network or the networks of third parties are prohibited. In particular, the following are strictly prohibited:

DoS/DDoS Attacks: Initiating, supporting, or participating in Denial of Service attacks (including: UDP Flood, TCP SYN Flood, HTTP Flood, Amplification Attacks, and others).

Scanning and Reconnaissance: Unauthorized port scanning (Port Scanning), vulnerability detection (Vulnerability Scanning), network mapping (Network Mapping), and the use of tools such as Zmap, Masscan, Nmap without the express, written consent of the target owner.

Network Identity Falsification (Spoofing): Forging IP/TCP/UDP packet headers (IP Spoofing), falsifying ARP records (ARP Poisoning), or DNS records (DNS Spoofing).

Routing Interference: Attempts to manipulate routing protocols (BGP, OSPF), announcing unauthorized IP prefixes (IP Hijacking).

Bypassing Security: Attempts to bypass authentication, authorization, or resource limiting mechanisms (Rate Limiting) of the Operator's systems.

High-Risk Anonymization:

a. Running TOR network exit nodes (Tor Exit Nodes) or similar services.
b. Operating open Proxy servers (Open Proxy) or public VPNs without traffic logging, or similar services.
c. Maintaining open DNS resolvers (Open DNS Resolvers) vulnerable to amplification attacks, or similar services.

§ 3. PROHIBITED CONTENT

It is prohibited to store, share, or link to content that violates Polish law, European Union law, or international law. This includes:

Illegal Content:

a. Child pornography (CSAM) and pedophilic content - **Reported immediately to law enforcement agencies (Interpol/Police).**
b. Content inciting terrorism, extremism, racial, ethnic, or religious hatred.
c. Instructions for manufacturing weapons, explosives, or drugs.

Copyright Infringement:

a. Illegal distribution of software, movies, music (Warez).

b. Public BitTorrent trackers or seedboxes sharing copyright-protected content.

Cybercrime:

a. Hosting Phishing sites (soliciting login data, card numbers).
b. "Scam" sites (fake investments, "grandparent" scams).
c. Distribution of malicious software (Malware, Ransomware, Spyware, Botnet C&C).
d. Hosting hacking tools ("Stresser", "Booter", Exploit Kits).

Violation of Personal Rights:

a. Doxxing (publishing private data of third parties without their consent).
b. Stalking, harassment, criminal threats.

§ 4. EMAIL POLICY

The Operator applies a Zero Tolerance policy for SPAM.

Port 25 Availability: Outgoing traffic on port 25 (SMTP) is blocked by default for security reasons. Unblocking it requires passing identity verification (KYC) in accordance with the Terms of Service.

Alternatives: Clients who do not wish to undergo KYC verification may use port 587 (SMTP Submission) with authentication, which is unblocked by default, or external SMTP services (e.g., Mailgun, SendGrid, Amazon SES, SparkPost).

SPAM Prohibition: Sending unsolicited commercial information (UCE/UBE) is prohibited. Every marketing e-mail must be sent exclusively to recipients who have given their consent (Double Opt-In).

Technical Requirements: Every mail server running on the Operator's infrastructure must have correctly configured records:

a. **rDNS (PTR):** Matching the host name (FQDN).
b. **SPF and DKIM:** Authenticating the sender.

IP Reputation: The Client is responsible for ensuring that the assigned IP address does not end up on blacklists (RBL), such as Spamhaus, Barracuda, SpamCop, or others.

Prohibited Practices:

a. Purchasing mailing lists.
b. Masking the sender's identity (Header Spoofing).
c. Using the Operator's servers to handle bounces from spam sent from another network.

§ 5. RESOURCE ABUSE

In order to ensure fair access to resources (Fair Share) for all Clients of the virtualization platform:

Crypto Mining:

a. ABSOLUTE PROHIBITION on using any resources (CPU, GPU, RAM, Storage) for mining virtual currencies (including: Bitcoin, Monero, and other similar ones).
b. The prohibition also applies to sharing computing power in distributed systems.

CPU Abuse:

a. **General Rule:** In order to ensure fair access to resources (Fair Share), actions causing **permanent performance degradation for other users** on the same physical node are prohibited.
b. **Monitoring:** The Operator monitors the "Steal Time" parameter. In the event that the Client's resource utilization causes Steal Time > 10% for other users for a period longer than 2 hours,

the Operator has the right to limit performance (Throttling) or contact the Client to optimize the load.

c. **Offer Exceptions:** The above restriction does not apply to dedicated servers or services promoted as "CPU unlimited" in the offer specification, provided this does not violate the prohibition on cryptocurrency mining.

d. **Prohibition of Artificial Loading:** Regardless of the offer, it is prohibited to run processes intended solely to generate artificial load (e.g., continuous benchmarks, stress-tests, looping scripts) without a justified business purpose.

Disk I/O Abuse: It is prohibited to generate continuous, extreme input/output operation loads (IOPS) that degrade the performance of the disk array (e.g., Chia plotting, intensive disk scanning, debug logging in a loop).

Consequences: The Operator's systems automatically monitor "Steal Time" and "I/O Wait" parameters. Exceeding the norms results in automatic performance limitation (Throttling), service restart, or service suspension.

§ 6. CLIENT RESPONSIBILITY AND SECURITY

6.1. Securing the Service: The Client is fully responsible for the security of their Service. This includes regular updates of the operating system and applications. A breach of the Client's Service due to a security vulnerability (e.g., old WordPress) and its use for an attack shall be charged to the Client's account.

6.2. Responsibility for Users (Reselling): If the Client resells the Operator's services to third parties (e.g., game hosting, shell accounts), they bear full responsibility for the actions of their users. The Client must have mechanisms in place allowing for the immediate blocking of their user who violates the regulations.

§ 7. ADMINISTRATIVE PENALTIES AND ABUSE PROCEDURE

In the event of an FUP violation, the Operator shall take the following steps:

7.1. Abuse Report: In the event of receiving a report of a violation, the Client is obliged to react and remove the cause within 24 hours (or 4 hours in critical matters).

7.2. Service Suspension: In the event of no reaction or a critical violation (DDoS, Mining, Phishing), the service is blocked immediately (Null-route/Suspend).

7.3. Amnesty Procedure (Second Chance):

a. In cases of unintentional violation (e.g., virus infection of the Client's service), the Operator may, as an exception, allow the service to be unblocked in accordance with the procedure described in the Terms of Service (Amnesty).

b. A necessary condition is the successful completion of identity verification (KYC) and consent to a complete reinstallation of the service (loss of data) in order to remove the threat.

7.4. Cost Recovery:

a. In the event of violations requiring technical intervention by the Operator (e.g., removing malicious software, RBL delisting procedure, analysis of advanced attacks), the Operator may charge the Client **justified administrative costs** proportional to the workload (hourly rate: 100 PLN/h), subject to a maximum amount of **300 PLN** per single incident.

b. Costs are collected exclusively in cases where the violation resulted from the Client's negligence or fault (e.g., failure to update the system, conscious spamming, maintaining unsecured services).

c. Costs are deducted from the vPLN Balance. In the absence of funds, the balance may take a

negative value, and the condition for lifting the block on services is the settlement of the underpayment (Wallet top-up).

7.5. Termination of Agreement: In the event of gross violations, the Operator terminates the agreement with immediate effect. Settlement issues are governed by the Terms of Service (Non-refundability of funds).

§ 8. FINAL PROVISIONS

8.1. FUP Changes: The Operator reserves the right to change this Fair Use Policy for important reasons (e.g., change in law, new security threats, infrastructure modernization). Clients will be informed of changes via e-mail or through a message in the Panel at least **30 days** in advance. Failure to object within this period constitutes acceptance of the changes. In the event of an objection, the Client has the right to terminate the agreement with immediate effect without incurring additional costs.

8.2. Integrity: In matters not regulated in the FUP, the provisions of the Terms of Service (TOS) shall apply.