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 " voxigames.com" domain name

This document is part of the set of documents:

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

Effective Date: 14.11.2026
Last Updated: 15.10.2026

§ 1. INITIAL PROVISIONS AND DEFINITIONS

1.1. Operator:

a. VoxiHost DANIEL MARSZAŁKOWSKI
b. ul. 3 Maja 29, 62-500 Konin, Poland
c. **NIP (Tax ID):** 6653080651 | REGON (National Business Registry): 542936383
d. **E-mail:** support@voxigames.com

operating the VoxiGames service (hereinafter referred to as "VoxiGames" 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 scope of the website available under the VoxiGames.com domain, the business activity of which is game server hosting. This document does not apply to other services, projects, or websites operated by the Operator under other 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 network reputation of the Operator.

1.5. Acceptance: Registration of an Account or ordering a Service is tantamount to full acceptance of this document and all related documents. In the event of changes to the FUP, the Client shall be notified 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 the event of non-acceptance of the changes.

1.6. Exclusive Discretion with Right of Appeal: The Operator reserves the right to make a technical and legal assessment of whether a given Client action 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 by submitting a ticket in the Support system. The appeal will be reviewed 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 activities that may disrupt the operation 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), regardless of whether the traffic is generated from the Client Panel, the Game Server itself, or mods and plugins installed thereon.

Scanning and Reconnaissance: Unauthorized Port Scanning, Vulnerability Scanning, Network Mapping, and the use of tools such as Zmap, Masscan, Nmap without the explicit, written consent of the target's owner.

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

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

Bypassing Security Measures: Attempts to bypass authentication, authorization, or resource limiting mechanisms (Rate Limiting) of the Operator's systems, including attempts to circumvent Anti-DDoS filters.

High-Risk Anonymization:

a. Running TOR network exit nodes (Tor Exit Nodes) or similar services.
b. Operating open proxies (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 forbidden to store, share, or link to content that violates Polish law, European Union law, or international law. This includes:

Illegal Content:

a. Child Sexual Abuse Material (CSAM) and pedophilic content - **Reported immediately to law enforcement authorities (Interpol/Police).**
b. Content inciting terrorism, extremism, racial, ethnic, or religious hatred.

c. Instructions for the manufacture of weapons, explosives, or drugs.

Copyright Infringement:

a. Illegal distribution of software, movies, music (Warez).
b. Public BitTorrent trackers or seedboxes sharing copyrighted content.
c. Distribution of illegal copies of games and sharing game client files on the Game Server in a manner that infringes the publisher's rights.

Cybercrime:

a. Hosting phishing websites (phishing for login credentials, card numbers).
b. "Scam" websites (fake investments, "granny scam" frauds).
c. Distribution of malicious software (Malware, Ransomware, Spyware, Botnet C&C).
d. Hosting hacking tools ("Stresser", "Booter", Exploit Kits).
e. Hosting "cracked" (pirated) game servers and distributing cheats and software that bypass game anti-cheat mechanisms (Anti-Cheat).

Infringement of Personal Rights:

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

§ 4. RESOURCE ABUSE PROTECTION

To ensure fair access to resources (Fair Share) for all Clients of the hosting platform:

Crypto Mining:

a. ABSOLUTE PROHIBITION of 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, as well as installing mods or plugins performing such calculations.

CPU Abuse:

a. **General Rule:** To ensure fair share access to resources, activities 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 a Client's resource utilization causes Steal Time > 10% for other users for a period longer than 2 hours, the Operator reserves the right to throttle performance (Throttling) or contact the Client in order to optimize the load.
c. **Offer Exceptions:** The above restriction does not apply to services promoted as "CPU unlimited" in the offer specification, provided it does not violate the crypto mining ban.
d. **Prohibition of Artificial Load:** Regardless of the offer, it is forbidden 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: Generating continuous, extreme input/output (IOPS) load that degrades disk array performance (e.g., intensive disk scanning, loop debug logging, excessive game world saves by a faulty plugin) is prohibited.

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

§ 5. GAME SERVER RULES

This section defines rules specific to game server hosting, supplementing the provisions of the Terms of Service (§ 4).

5.1. Prohibition of Hosting Attack Tools: It is forbidden to use the Game Server to host, run, or distribute stressers, booters, DDoS panels, and any software used to generate attack traffic.

5.2. Prohibition of Acting as a Proxy/Relay: It is forbidden to use the Game Server as a proxy, open relay, or traffic amplifier (in accordance with § 2).

5.3. Slot and Resource Limits: It is forbidden to bypass slot limits and resource limits (RAM, CPU, disk) assigned to the purchased Service, in particular by modifying server software, running additional processes outside the panel, or installing mods that artificially increase server capacity.

5.4. Mods and Plugins: The Client bears sole responsibility for the legality, origin, and security of installed mods and plugins (in accordance with TOS § 4.5). An outdated or infected plugin constitutes an attack vector and burdens the Client's account - even if it is used to attack other entities.

5.5. Compliance with Game Publisher EULA: It is forbidden to use the Game Server for activities inconsistent with the game publisher's End User License Agreement (EULA), in particular hosting pirated servers and distributing materials that infringe the publisher's rights (in accordance with TOS § 4.6).

5.6. Liability for End Players: The Client is liable for the actions of End Players on their Game Server to the same extent as for their own actions (in accordance with TOS § 4.12).

§ 6. CLIENT LIABILITY AND SECURITY

6.1. Service Security: The Client is fully responsible for the security of their Service. This includes regular updates of game server software, mods, and plugins, as well as changing access passwords (Game Panel, SFTP/FTP, database). A breach of the Client's Service due to a security vulnerability (e.g., an outdated plugin) and its use to carry out an attack shall burden the Client's account.

6.2. Liability for Users (Reselling): If the Client resells the Operator's services to third parties (e.g., reselling game server slots, sharing access with co-admins), they bear full liability for the actions of their users. The Client must have mechanisms in place enabling 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 violation report, the Client is obliged to react and remove the cause within 24 hours (or 4 hours in critical matters).

7.2. Service Blockade: In the absence of a reaction or in the event of 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., viral infection of the Client's service), the Operator may, as an exception, permit the unblocking of the service in accordance with the procedure described in the Terms of Service (Amnesty).

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

7.4. Cost Recovery:

a. In the event of violations requiring the Operator's technical intervention (e.g., malware

removal, RBL delisting procedure, analysis of advanced attacks), the Operator may charge the Client with **reasonable administrative costs** proportional to the workload (hourly rate: 100 EUR/h), subject to a maximum amount of **300 EUR** per single incident.

b. Costs are charged exclusively in cases where the violation resulted from the Client's omission or fault (e.g., failure to update mods, intentional spamming, maintaining unsecured services).

c. Costs are deducted from the Credits Balance. In the absence of funds, the balance may become negative, and a condition for lifting the blockade on services is settling the shortfall (topping up the Wallet).

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 Amendments: The Operator reserves the right to amend this Fair Use Policy for important reasons (e.g., change of law, new security threats, infrastructure modernization). Clients will be informed about the amendments via email or through a message in the Panel at least **30 days** in advance. Failure to object within this period constitutes acceptance of the amendments. 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.