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.

TERMS OF SERVICE (TOS)

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 Usage Policy (FUP)

Effective Date: 14.02.2026
Last Updated: 15.01.2026

§ 1. 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. Client: A person using the Services. This may be:

a. A natural person of legal age or a natural person who has reached the age of 16 and obtained the consent of a legal representative (parent/guardian).
b. A legal person (e.g., a Limited Liability Company).
c. An organizational unit without legal personality (e.g., an association).

1.3. Consumer: A natural person using the Services for purposes unrelated to their business or professional activity (e.g., a Client purchasing a server for a private project/game).

1.4. Digital Service: A service provided by the Operator electronically, consisting of the provision, processing, or storage of data in digital form (e.g., VPS Server, Game Server, Web Hosting, Backup Space).

1.5. vPLN (Virtual Wallet/Service Points): vPLN is digital content within the meaning of Art. 2 point 5 of the Consumer Rights Act, acquired through an agreement for the supply of digital content. It constitutes an electronic voucher that can be exchanged for Digital Services offered by the Operator. vPLN has no payment value outside the VoxiHost ecosystem. It is not electronic money (within the meaning of the Payment Services Act, Art. 2 point 21a) nor a financial instrument. The acquisition of vPLN means the immediate delivery of digital content to the Client's Wallet. **vPLN funds are not subject to exchange for cash, withdrawal, or transfer to other persons.**

1.6. Payment Operator: An external entity providing online payment intermediation services to the Operator and the Client (e.g., transfers, cards, BLIK). The Payment Operator is the exclusive administrator of the Client's data regarding payments and is subject to separate regulations and privacy policies.

1.7. Regulations/TOS: This document specifying the rules for the provision of Services.

1.8. Client Panel/Service: The platform available at VoxiHost.pl, through which the Client manages Services and the Account.

1.9. Account: The Client's individual account in the Client Panel, enabling access to and management of Services.

1.10. Agreement: The agreement concluded between the Operator and the Client, including:

a. An agreement for the supply of digital content (vPLN), concluded at the time of topping up the Wallet,

b. An agreement for the provision of Digital Services (VPS, Hosting, etc.), concluded at the time of activating the Service using vPLN funds.

1.11. Billing Period: A unit of time (month, year) for which the remuneration for the Service is collected.

1.12. Related Documents: The set of documents regulating the cooperation between the Operator and the Client, listed in the header of this document.

1.13. Parties: The Operator and the Client, collectively referred to as the Parties to the Agreement.

1.14. Abuse: Using the Services in a manner that violates the law, the Regulations, or the rights of third parties, in particular:

a. sending spam,

b. DDoS attacks,

c. phishing,

d. hosting illegal content,

e. copyright infringement,

f. attempts to break into other systems.

1.15. Fraud: An action aimed at obtaining Services or funds by deception, including:

a. payments with a stolen credit card,

b. unjustified Chargeback,

c. impersonating another person,

d. falsifying verification documents.

§ 2. PRELIMINARY PROVISIONS

2.1. Availability of Regulations: The Regulations and Related Documents are available free of charge on the VoxiHost.pl home page in the footer and in the Client Panel after logging in, in a form that allows for downloading, saving, and printing. The Operator makes the Regulations available before the conclusion of the agreement and at every request of the Client.

2.2. Scope of Application: These Terms of Service constitute an integral part of the set of Related Documents and apply exclusively within the website available under the VoxiHost.pl domain. This document does not apply to other websites, projects, or web pages managed by the Operator under other addresses.

2.3. Integrity: These Regulations constitute an integral part of the Related Documents.

2.4. Purpose: The purpose of the Regulations is to define the general rules of cooperation, the rights and obligations of the Parties, and the rules for providing Digital Services electronically.

2.5. Acceptance: Registration of an Account or ordering a Service is equivalent to full acceptance of the Regulations and all Related Documents. In the event of changes to the Regulations or Related Documents, the Client will be informed in accordance with §9.1. Lack of objection within 30 days of notification means acceptance of the changes. The Client has the right to terminate the agreement in case of non-acceptance of changes without incurring additional costs.

2.6. Legal Basis: The Regulations comply with applicable Polish and EU law, in particular with:

a. The Act of 23 April 1964 - Civil Code,
b. The Act of 30 May 2014 on consumer rights,
c. The Act of 18 July 2002 on the provision of electronic services,
d. Regulation (EU) 2016/679 (GDPR),
e. Regulation (EU) 2022/2065 (DSA).

2.7. Technical Requirements: To use the Services, it is necessary to have a device with Internet access, a correctly configured web browser (e.g., Chrome, Firefox) supporting Cookies and JavaScript, and an active e-mail account.

§ 3. USER ACCOUNT AND SECURITY

3.1. Registration: A condition for using the Services is creating an Account on the website. **Registration is free of charge.** Persons aged 16-18 are required to obtain the consent of a legal representative (parent/guardian). If the Client indicates an age below 18, the Operator will contact them to verify the consent of the legal representative.

3.2. Security of Login Data:

a. The Client is obliged to keep Account access data confidential and to use appropriate security measures (strong password of at least 12 characters with uppercase and lowercase letters, numbers, and special characters, 2FA).
b. **Towards Clients who are not Consumers:** The Operator is not liable for damages resulting from sharing login data with third parties or their theft due to the Client's negligence (e.g., using the password "123456", "password", saving the password in unencrypted form in a text file on the desktop, sharing the password with an employee without supervision).
c. **Towards Consumers:** The Operator is liable in accordance with the general principles of the Civil Code. The exclusion of liability applies only to damages resulting from gross negligence or intentional action of the Consumer. Gross negligence is considered, in particular:
    i. consciously sharing the password with unauthorized persons,
    ii. providing login data in response to a phishing message despite clear warnings,
    iii. using the same password as for other services that have previously leaked (available in

breach databases),

iv. intentionally disabling 2FA despite previous activation while being aware of the risk.

The Operator is not liable for damages resulting from hacker attacks exploiting vulnerabilities in the Client's device (e.g., keylogger, trojan), provided that the Operator has demonstrated due diligence in securing the infrastructure on its side.

3.3. Single Account Principle: It is forbidden to create multiple accounts by one Client (Multi-accounts) without a justified business reason. It is permitted to have: one personal Account (as a natural person/consumer) and one business Account (as an entrepreneur), provided they are linked to different e-mail addresses and serve separate purposes. Creating additional accounts requires the Operator's consent.

3.4. Identity Verification (KYC):

a. **Purpose of verification:** The Operator may require identity verification to prevent abuse, fraud, and to protect the infrastructure against criminal activities, in particular when:
   i. unlocking High-Risk Services (port 25/SMTP, IRC, UDP),
   ii. accessing Test Services (Trial),
   iii. suspicion of violation of the Regulations or criminal activities,
   iv. "Amnesty" procedure (unlocking a service after a violation).

b. **Verification Processor:** Identity verification is carried out by an external entity didit.me (https://didit.me), which acts as an independent personal data controller regarding the verification process. didit.me processes verification data (identity documents, selfies) solely for the purpose of confirming identity.

c. **Scope of processing by the Operator:** The Operator receives from didit.me only:
   i. the verification result (positive/negative),
   ii. access to verification data for a maximum period of 1 month to verify the authenticity of the process and generate its own cryptographic hash of the document data (irreversible, SHA-256/bcrypt), which the Operator stores locally.

d. After 1 month, the Operator stores only the verification status, verification date, and the cryptographic hash of the document data.

e. **Legal basis:** Processing the verification result: Art. 6(1)(b) GDPR (performance of the contract). Storing the hash: Art. 6(1)(f) GDPR (legitimate interest in preventing re-registration of persons blocked for serious violations).

f. **Right to object:** The Client has the right to refuse KYC verification. In such a case, the Operator may refuse to provide High-Risk Services, Test Services, and the Amnesty procedure (unlocking the service after a violation of the Regulations).

3.5. Risk Assessment and Refusal of Service: The Operator reserves the right to refuse registration, service activation, or to block an Account in the event of obtaining reliable information indicating a high risk to infrastructure security, in particular when:

a. The Client is on a list of persons/entities associated with cybercrime,

b. registration data is false or stolen,

c. the Client was previously blocked for serious violations,

d. there is a reasonable suspicion of using services for criminal activities.

Towards Consumers: The Operator will inform about the reasons for refusal/blocking and enable the submission of explanations within 14 days. The Operator will consider the explanations within 7 business days and inform the Client of the final decision. If the refusal is maintained, the Consumer has the right to file a complaint (§7.2) and use out-of-court dispute resolution.

Towards Clients who are not Consumers: The Operator is not obliged to justify the decision.

3.6. Communication Culture: The Parties undertake to conduct communication (Support, E-mail) in a cultured manner based on mutual respect and understanding. The Operator does not tolerate verbal aggression, profanity, or threats directed at the staff. A gross violation of the rules of personal culture is considered, in particular:

a. punishable threats (Art. 190 of the Penal Code),
b. insults (Art. 216 of the Penal Code),
c. repeated (more than 3 times in one conversation) use of profanity of an invective nature towards employees despite a prior warning,
d. harassment of employees (more than 5 reports of the same case within 24 hours).

Profanity is understood as words commonly considered offensive (vulgar epithets, swear words). The Operator applies common sense and takes into account the emotional context (stress related to service failure).

In the event of a gross violation, the Operator reserves the right to temporarily suspend the processing of reports from a given Client (up to 7 days). In the event of a repeated violation - to terminate the agreement.

3.7. Account Ownership Disputes:

a. The Operator does not resolve property disputes between partners, employees, or third parties regarding access to the Account.
b. The only person considered the disposer of the Account is the person who has access to the authorized e-mail address and the 2FA method.

3.8. Account Blocking and Deletion: The Operator has the right to block or delete an Account in the event of a gross violation of the Regulations, Related Documents, or acting to the detriment of the infrastructure.

3.9. Recidivism Prevention (Infrastructure Protection System): In the event of a permanent Account block for serious violations (Abuse, Fraud), the Operator applies technical and organizational mechanisms to prevent the re-registration of persons committing serious violations. These mechanisms may include, among others, the storage of anonymized verification data (e.g., cryptographic hash), which prevent the reversal of the process and identification of the person but allow for the automatic detection of a re-registration attempt. Legal basis: Art. 6(1)(f) GDPR (Operator's legitimate interest in protecting the infrastructure against recidivists). Anonymized data may be stored for a period of up to 10 years from the date of the block or until the Operator's legal interest in storing them ceases.

3.10. Amnesty:

a. In the event of a service block for violation of the Regulations, the Client may be granted a one-time opportunity to unlock resources, provided they pass the KYC procedure.
b. The procedure involves **restoring the service to factory settings (reinstallation and loss of data).**
c. **Towards Consumers:** The Operator provides a 14-day period to decide on KYC verification before permanent data deletion.
d. Refusal of verification results in maintaining the block and termination of the agreement.

3.11. Inactive Accounts: The Operator reserves the right to permanently delete an Account that the Client has not logged into for a period of 36 months and which does not have any active Services. Before deleting the Account, the Operator will send a warning to the Client's e-mail address with a 60-day deadline to log into the Panel (which will extend the Account's validity) or use vPLN funds to purchase Services. The Operator will make at least two contact attempts (e-mail + SMS, if

available). In the absence of a reaction within 60 days, the Account will be deleted, and the accumulated vPLN funds will be converted into a unique promotional code without an expiration date, which will be sent to the Client's e-mail address and can be used upon re-registration on the website.

§ 4. PAYMENTS AND VIRTUAL WALLET (VPLN)

4.1. Billing Model: Services are provided in a prepaid model (paid in advance) based on a virtual wallet (vPLN). The Client first acquires vPLN points (digital content) and then exchanges them for Digital Services.

4.2. Virtual Wallet (vPLN):

a. Purchase of Services is possible only using vPLN points accumulated in the Virtual Wallet.

b. Topping up the Wallet occurs through Payment Operators (transfers, cards, BLIK).

c. The detailed legal definition of vPLN is contained in §1.5 above.

4.3. No Refunds (Non-refundability):

vPLN Top-up (Digital Content):

a. Due to the nature of the provision (immediate delivery of digital content in the form of vPLN points), vPLN funds are non-refundable.

b. A condition for topping up is the Consumer's consent to start the delivery of digital content before the deadline for withdrawal from the agreement and acknowledgment of the loss of the right of withdrawal (in accordance with Art. 38 point 13 of the Consumer Rights Act).

c. Consent is expressed by checking a statement in the Client Panel before making the top-up.

Digital Service Activation (VPS, Hosting, etc.):

a. Digital Services are activated immediately after purchase using vPLN funds.

b. A condition for activation is the Consumer's consent to the immediate commencement of the digital service provision before the deadline for withdrawal from the agreement and acknowledgment of the loss of the right of withdrawal (in accordance with Art. 38 point 13 of the Consumer Rights Act).

c. Consent is expressed by checking a statement in the Client Panel before activating the Service.

Lack of consent:

Without expressing the above consents, topping up or activating the Service, respectively, is not possible.

4.4. Renewal of Services:

a. Renewal of services is done manually by the Client. **The system does not collect fees automatically.**

b. Failure to pay results in suspension of the service. **After 7 days, the service is permanently deleted** along with the data saved within that Service (files, databases, configuration) in an irreversible manner, in accordance with GDPR security procedures. The Account in the Client Panel remains active.

4.5. Sales Documents: The Operator issues invoices (without VAT) or bills only at the Client's request submitted through the Panel or to the address support@voxihost.pl.

4.6. Chargeback and Frauds:

a. Initiation by the Client of a payment reversal procedure (Chargeback/Dispute) with the Payment Operator results in **automatic Account suspension** until the matter is clarified. If

the Chargeback turns out to be unjustified (the Client received vPLN according to the order and yet reversed the payment), the Operator has the right to **terminate the agreement with immediate effect** and seek compensation (including dispute handling costs) through civil law and refer the case for debt collection (if the dispute value exceeds 1000 PLN).

b. In the case of an unjustified chargeback with a value below 1000 PLN, the Operator reserves the right to report the incident to anti-fraud systems (databases of blocked users) and refuse to provide services in the future to this Client or other accounts linked to their verification data.

c. Detection of payment with a stolen credit card results in immediate reporting of the case to law enforcement authorities.

4.7. Pricing and Offer Errors:

a. The Operator makes efforts to ensure that the prices and descriptions of Services are correct; however, it reserves the right to correct obvious clerical or system errors (e.g., a price of 0 PLN for a paid service).

b. In the case of an order placed based on an incorrect price, the Operator has the right to cancel the transaction and refund the vPLN funds.

4.8. Affiliate Program (Affiliation): It is forbidden to use affiliate mechanisms to obtain benefits from one's own purchases (so-called Self-referral) or to create fictitious accounts to obtain commissions. Violation results in the forfeiture of accumulated affiliate funds.

§ 5. RIGHTS AND OBLIGATIONS OF THE PARTIES

5.1. Obligations of the Operator:

a. The Operator undertakes to provide Services with due professional diligence.

b. The Operator ensures the availability of infrastructure (hardware, network, power) at the level specified in the SLA.

c. The Operator has the right to conduct maintenance work (Maintenance), which may cause temporary unavailability of Services. Detailed rules regarding maintenance work (including advance notification) are specified in document SLA §4.1.

5.2. Obligations of the Client:

a. The Client undertakes to use the Services in a manner consistent with the law, the Regulations, and good practices.

b. The Client is responsible for the ongoing update of their contact details in the Panel.

c. The Client is forbidden from taking actions that could disrupt the operation of the Operator's infrastructure (e.g., reverse engineering, penetration tests without consent).

d. The Client bears full responsibility for all content, files, and applications placed within the provided resources (Services).

5.3. Exclusion of Liability: The Operator is not liable for damages resulting from:

a. **force majeure, including:** natural disasters (flood, fire, earthquake), acts of war, riots, strikes, terrorist attacks, epidemics/pandemics (including administrative restrictions related to COVID-19 or similar public health threats), national or regional power grid failures,

b. failures on the part of Internet connection providers (outside the Operator's network),

c. incorrect software configuration by the Client (e.g., blocking one's own SSH access),

d. DDoS attacks directed at the Client's IP address,

e. loss of data for reasons attributable to the Client (lack of backups, incorrect configuration, intentional deletion) or for reasons independent of the Operator (hardware failure despite redundancy, force majeure).

Towards Consumers: The Operator is liable for data loss if it is proven that the damage resulted from the Operator's intentional fault or gross negligence. The Client is obliged to have their own backup copy of the data.

Towards Clients who are not Consumers: The Operator's liability for lost profits (lucrum cessans - lost profits) and for data loss is excluded (the Client bears exclusive responsibility for backups).

5.4. Indemnification (Cost Coverage):

a. **Towards Clients who are not Consumers:** The Client undertakes to cover reasonable costs (including legal assistance costs and compensation) that the Operator would incur in connection with third-party claims resulting from the Client's unlawful use of the Services (e.g., copyright infringement, attacking other networks, hosting phishing), provided that the Operator demonstrates a causal link and the amount of damage.

b. **Towards Consumers:** The above provision does not apply. The Consumer's liability is regulated by the general principles of the Civil Code.

5.5. Software Licenses:

a. The Client bears exclusive responsibility for the legality of the software installed and used within the Operator's infrastructure (e.g., Windows Server licenses, cPanel, DirectAdmin, third-party software).

b. The Operator, as an infrastructure provider, does not verify the licenses held by the Client; however, in the event of receiving a reliable report of a violation (e.g., from Microsoft, Adobe), it has the right to suspend the service until the licensing status is clarified.

5.6. IP Addressing and Migrations:

a. IP addresses assigned to the Service remain the property of the Operator (or its providers). The Client only receives the right to their temporary use.

b. The Operator reserves the right to change the assigned IP address in justified technical cases (e.g., change of server room, network reorganization), informing the Client in advance. An IP change does not constitute a basis for a complaint.

5.7. Scope of Support (Unmanaged):

a. Unless a dedicated administrative service has been purchased, the Operator's services are Unmanaged (Managed by the Client).

b. The Operator's Technical Support covers only the operation of the infrastructure (network availability, power, panel operation, hardware restart).

c. **The Operator does not provide support for the configuration of the operating system by the Client, installation of applications**, fixing errors in the Client's scripts, or teaching how to use Linux/Windows systems.

d. Detailed rules for the availability of Technical Support (including Working Hours and Response Time) are specified in the SLA document.

e. **Automatic Support (Assistant):** The Operator provides automatic systems that, based on the content of the report, suggest proven solutions from the Knowledge Base. The Client acknowledges that the automatic selection of instructions may not take into account the specifics of an unusual problem and should be treated as auxiliary.

5.8. Backup and Snapshot Service:

a. In the event of purchasing an additional backup service (Backup/Snapshot), the Operator will make efforts to ensure that copies are made according to the schedule.

b. This service is auxiliary and does not exempt the Client from the obligation to have an independent copy of data outside the Operator's infrastructure. The Operator is not liable for data consistency within the copy (e.g., database corruption during a dump) or for a backup

system failure.

5.9. Experimental Services (BETA): The Operator may provide functionalities marked as "BETA". These services may be unstable and are not covered by the SLA guarantee. The Client uses them at their own risk.

5.10. Limitation of Liability: The Operator's total compensatory liability towards a Client who is not a Consumer is limited in each case to the amount of the monthly fee for the given Service from which the damage results. The limitation does not apply to damages caused intentionally or as a result of gross negligence.

5.11. Liability for Third Parties: The Client bears full responsibility for the actions and omissions of third parties to whom they have made their Services available (e.g., employees, associates, their end customers), as for their own actions.

5.12. Technological Evolution: The Operator reserves the right to change the technical parameters of the Services (e.g., hardware update, software version change) in order to improve security and performance, provided that this does not deteriorate the overall functionality of the Service.

5.13. Legal Support in Abuse Cases: In the event that the Client receives a legal request (summons, lawsuit) from a third party regarding content or actions within the Service provided by the Operator, and the Client believes that the allegations are groundless, the Operator may - at the Client's request - provide basic technical information (logs, incident information) necessary for the Client's defense. The Operator does not provide legal services nor bear the costs of the Client's defense.

§ 6. DSA PROCEDURES (DIGITAL SERVICES ACT) AND ABUSE

6.1. Legal Basis (DSA): Whenever DSA is mentioned, it is understood as Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act).

6.2. Contact Point for Authorities:

a. For the authorities of Member States, the European Commission, and the European Board for Digital Services, a contact point is designated: daniel@voxihost.pl.

b. Communication is conducted in Polish or English.

6.3. Reporting Illegal Content (Abuse):

a. Any person may report the presence of illegal content in the Operator's infrastructure to the address: abuse@voxihost.pl.

b. **The report must contain:**

i. a justification,

ii. the location of the content (URL/IP),

iii. the reporter's data (unless it concerns sexual offenses against children),

iv. a statement of good faith.

6.4. Blocking Decisions:

a. In the event of blocking a service due to a violation of the law or the Regulations, the Operator will provide the Client with a statement of reasons for the decision (in accordance with DSA requirements