POLITYKA UCZCIWEGO KORZYSTANIA (FUP)

Dla platformy/strony/serwisu/usług znajdującego/znajdujących się pod adresem domeny " voxihost.pl"

Niniejszy dokument jest częścią zbioru dokumentów:

a. Regulamin Usług (TOS)
b. Polityka Prywatności (PP)
c. Umowa o Gwarantowanym Poziomie Świadczenia Usług (SLA)
d. Polityka Uczciwego Korzystania (FUP)

Data Wprowadzenia: 14.02.2026

Data Aktualizacji: 15.01.2026

§ 1. POSTANOWIENIA WSTĘPNE I DEFINICJE

1.1. Operator:

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

(dalej zwany "VoxiHost" lub "Operatorem").

1.2. Zakres Obowiązywania: Niniejsza Polityka Uczciwego Korzystania stanowi integralną część Regulaminu Usług i obowiązuje wyłącznie w ramach serwisu internetowego dostępnego pod domeną VoxiHost.pl. Dokument ten nie ma zastosowania do innych serwisów, projektów czy stron internetowych prowadzonych przez Operatora pod innymi adresami.

1.3. Integralność: Niniejsza Polityka Uczciwego Korzystania stanowi integralną część zbioru dokumentów wymienionych w nagłówku niniejszego dokumentu.

1.4. Cel: Celem Polityki Uczciwego Korzystania jest zapewnienie stabilności, bezpieczeństwa i wysokiej wydajności infrastruktury dla wszystkich Klientów oraz ochrona reputacji sieciowej Operatora.

1.5. Akceptacja: Rejestracja Konta lub zamówienie Usługi jest równoznaczne z pełną akceptacją niniejszego dokumentu oraz wszystkich dokumentów powiązanych. W przypadku wprowadzenia zmian w FUP, Klient zostanie poinformowany zgodnie z §8.1. Brak sprzeciwu w terminie 30 dni od powiadomienia oznacza akceptację zmian. Klient ma prawo wypowiedzieć umowę w przypadku braku akceptacji zmian.

1.6. Wyłączne Uznanie z Prawem Odwołania: Operator zastrzega sobie prawo do oceny technicznej i prawnej, czy dane działanie Klienta stanowi naruszenie niniejszej Polityki. W przypadku decyzji o blokadzie lub nałożeniu ograniczeń, Klient ma prawo odwołać się od decyzji w ciągu 7 dni poprzez zgłoszenie w systemie Support (ticket). Odwołanie zostanie rozpatrzone przez niezależnego członka zespołu technicznego w ciągu 7 dni roboczych. Decyzja w wyniku odwołania jest ostateczna.

§ 2. BEZPIECZEŃSTWO SIECI I INFRASTRUKTURY (NETWORK ABUSE)

Zabrania się wszelkich działań mogących zakłócić funkcjonowanie sieci Operatora lub sieci podmiotów trzecich. W szczególności surowo zabronione są:

Ataki DoS/DDoS: Inicjowanie, wspieranie lub uczestnictwo w atakach typu Denial of Service (w tym: UDP Flood, TCP SYN Flood, HTTP Flood, Amplification Attacks, i innych).

Skanowanie i Rekonesans: Nieautoryzowane skanowanie portów (Port Scanning), wykrywanie podatności systemów (Vulnerability Scanning), mapowanie sieci (Network Mapping) oraz używanie narzędzi typu Zmap, Masscan, Nmap bez wyraźnej, pisemnej zgody właściciela celu.

Fałszowanie Tożsamości Sieciowej (Spoofing): Preparowanie nagłówków pakietów IP/TCP/UDP (IP Spoofing), fałszowanie rekordów ARP (ARP Poisoning) lub DNS (DNS Spoofing).

Ingerencja w Routing: Próby manipulacji protokołami routingu (BGP, OSPF), ogłaszanie nieautoryzowanych prefiksów IP (IP Hijacking).

Omijanie Zabezpieczeń: Próby omijania mechanizmów uwierzytelniania, autoryzacji lub limitowania zasobów (Rate Limiting) systemów Operatora.

Anonimizacja Wysokiego Ryzyka:

a. Uruchamianie węzłów wyjściowych sieci TOR (Tor Exit Nodes), bądź usług podobnych.
b. Prowadzenie otwartych serwerów Proxy (Open Proxy) lub publicznych VPN bez logowania ruchu, bądź usług podobnych.
c. Utrzymywanie otwartych resolverów DNS (Open DNS Resolvers) podatnych na ataki amplifikacyjne, bądź usług podobnych.

§ 3. NIEDOZWOLONE TREŚCI (PROHIBITED CONTENT)

Zabrania się przechowywania, udostępniania lub linkowania do treści, które naruszają prawo polskie, prawo Unii Europejskiej lub prawo międzynarodowe. Obejmuje to:

Treści Nielegalne:

a. Pornografia dziecięca (CSAM) oraz treści pedofilskie - **Zgłaszane natychmiast do organów ścigania (Interpol/Policja).**
b. Treści nawołujące do terroryzmu, ekstremizmu, nienawiści rasowej, etnicznej lub religijnej.
c. Instrukcje wytwarzania broni, materiałów wybuchowych lub narkotyków.

Naruszenie Praw Autorskich:

a. Nielegalna dystrybucja oprogramowania, filmów, muzyki (Warez).
b. Publiczne trackery BitTorrent lub seedboxy udostępniające treści chronione prawem autorskim.

Cyberprzestępczość:

a. Hosting stron Phishingowych (wyłudzanie danych logowania, numerów kart).
b. Strony typu "Scam" (fałszywe inwestycje, oszustwa "na wnuczka").
c. Dystrybucja złośliwego oprogramowania (Malware, Ransomware, Spyware, Botnet C&C).
d. Hosting narzędzi hakerskich ("Stresser", "Booter", Exploit Kits).

Naruszenie Dóbr Osobistych:

a. Doxxing (publikowanie prywatnych danych osób trzecich bez ich zgody).
b. Stalking, nękanie, groźby karalne.

§ 4. ZASADY DOTYCZĄCE POCZTY ELEKTRONICZNEJ (EMAIL POLICY)

Operator stosuje politykę Zero Tolerancji dla SPAM-u.

Dostępność Portu 25: Ruch wychodzący na porcie 25 (SMTP) jest domyślnie zablokowany ze

względów bezpieczeństwa. Jego odblokowanie wymaga przejścia weryfikacji tożsamości (KYC) zgodnie z Regulaminem Usług.

Alternatywy: Klienci, którzy nie chcą przechodzić weryfikacji KYC, mogą korzystać z portu 587 (SMTP Submission) z uwierzytelnieniem, który jest odblokowany domyślnie, lub z zewnętrznych usług SMTP (np. Mailgun, SendGrid, Amazon SES, SparkPost).

Zakaz SPAM-u: Zabrania się wysyłania niezamówionej informacji handlowej (UCE/UBE). Każdy e-mail marketingowy musi być wysyłany wyłącznie do odbiorców, którzy wyrazili na to zgodę (Double Opt-In).

Wymogi Techniczne: Każdy serwer pocztowy uruchomiony na infrastrukturze Operatora musi posiadać poprawnie skonfigurowane rekordy:

a. **rDNS (PTR):** Zgodny z nazwą hosta (FQDN).
b. **SPF i DKIM:** Uwierzytelniające nadawcę.

Reputacja IP: Klient odpowiada za to, aby przydzielony adres IP nie trafił na czarne listy (RBL), takie jak Spamhaus, Barracuda, SpamCop, bądź inne podobne.

Zakazane Praktyki:

a. Kupowanie baz adresowych.
b. Maskowanie tożsamości nadawcy (Header Spoofing).
c. Używanie serwerów Operatora do obsługi zwrotek (Bounces) ze spamu wysyłanego z innej sieci.

§ 5. OCHRONA ZASOBÓW SYSTEMOWYCH (RESOURCE ABUSE)

W celu zapewnienia sprawiedliwego dostępu do zasobów (Fair Share) dla wszystkich Klientów platformy wirtualizacyjnej:

Kopanie Kryptowalut (Crypto Mining):

a. BEZWZGLĘDNY ZAKAZ wykorzystywania jakichkolwiek zasobów (CPU, GPU, RAM, Storage) do wydobywania walut wirtualnych (w tym: Bitcoin, Monero i innych podobnych).
b. Zakaz dotyczy również udostępniania mocy obliczeniowej w systemach rozproszonych.

Obciążenie Procesora (CPU Abuse):

a. **Zasada Ogólna:** W celu zapewnienia sprawiedliwego dostępu do zasobów (Fair Share), zabrania się działań powodujących **trwałą degradację wydajności dla innych użytkowników** na tym samym węźle fizycznym.
b. **Monitoring:** Operator monitoruje parametr "Steal Time". W przypadku, gdy wykorzystanie zasobów przez Klienta powoduje Steal Time > 10% dla innych użytkowników przez okres dłuższy niż 2 godziny, Operator ma prawo do ograniczenia wydajności (Throttling) lub kontaktu z Klientem w celu optymalizacji obciążenia.
c. **Wyjątki Ofertowe:** Powyższe ograniczenie nie dotyczy serwerów dedykowanych bądź usług promowanych jako "CPU unlimited" w specyfikacji oferty, o ile nie narusza to zakazu kopania kryptowalut.
d. **Zakaz Sztucznego Obciążania:** Niezależnie od oferty, zabrania się uruchamiania procesów służących wyłącznie generowaniu sztucznego obciążenia (np. ciągłe benchmarki, stress-testy, skrypty pętlujące) bez uzasadnionego celu biznesowego.

Obciążenie Dysku (Disk I/O Abuse): Zabrania się generowania ciągłego, ekstremalnego obciążenia operacjami wejścia/wyjścia (IOPS), które degradują wydajność macierzy dyskowej (np. Chia plotting, intensywne skanowanie dysku, logowanie debugowania w pętli).

Konsekwencje: Systemy Operatora automatycznie monitorują parametry "Steal Time" i "I/O Wait". Przekroczenie norm skutkuje automatycznym ograniczeniem wydajności (Throttling), restartem usługi lub zablokowaniem usługi.

§ 6. ODPOWIEDZIALNOŚĆ I BEZPIECZEŃSTWO KLIENTA

6.1. Zabezpieczenie Usługi: Klient jest w pełni odpowiedzialny za bezpieczeństwo swojej Usługi. Obejmuje to regularne aktualizacje systemu operacyjnego i aplikacji. Włamanie do Usługi Klienta z powodu luki w zabezpieczeniach (np. stary WordPress) i wykorzystanie jej do ataku obciąża konto Klienta.

6.2. Odpowiedzialność za Użytkowników (Reselling): Jeśli Klient odsprzedaje usługi Operatora osobom trzecim (np. hosting gier, konta shell), ponosi pełną odpowiedzialność za działania swoich użytkowników. Klient musi posiadać mechanizmy umożliwiające natychmiastowe zablokowanie swojego użytkownika łamiącego regulamin.

§ 7. KARY ADMINISTRACYJNE I PROCEDURA ABUSE

W przypadku naruszenia FUP, Operator podejmuje następujące kroki:

7.1. Zgłoszenie Abuse: W przypadku otrzymania zgłoszenia o naruszeniu, Klient ma obowiązek zareagować i usunąć przyczynę w ciągu 24 godzin (lub 4 godzin w sprawach krytycznych).

7.2. Blokada Usługi: W przypadku braku reakcji lub naruszenia krytycznego (DDoS, Mining, Phishing), usługa jest blokowana natychmiast (Null-route/Suspend).

7.3. Procedura Amnestii (Druga Szansa):

a. W przypadkach niesumyślnego naruszenia (np. infekcja wirusowa usługi Klienta), Operator może, na zasadzie wyjątku, zezwolić na odblokowanie usługi zgodnie z procedurą opisaną w Regulaminie Usług (Amnestia).

b. Warunkiem koniecznym jest pomyślne przejście weryfikacji tożsamości (KYC) oraz zgoda na całkowitą reinstalację usługi (utratę danych) w celu usunięcia zagrożenia.

7.4. Zwrot Kosztów (Cost Recovery):

a. W przypadku naruszeń wymagających interwencji technicznej Operatora (np. usuwanie złośliwego oprogramowania, procedura delisting z RBL, analiza zaawansowanych ataków), Operator może obciążyć Klienta **uzasadnionymi kosztami administracyjnymi** proporcjonalnymi do nakładu pracy (stawka godzinowa: 100 PLN/h), z zastrzeżeniem maksymalnej kwoty **300 PLN** za pojedyncze zdarzenie.

b. Pobieranie kosztów następuje wyłącznie w przypadkach, gdy naruszenie wynikało z zaniechania lub winy Klienta (np. brak aktualizacji systemu, świadome spamowanie, utrzymywanie niezabezpieczonych usług).

c. Koszty są pobierane z Salda vPLN. W przypadku braku środków, saldo może przyjąć wartość ujemną, a warunkiem zdjęcia blokady z usług jest uregulowanie niedopłaty (doładowanie Portfela).

7.5. Rozwiązanie Umowy: W przypadku rażących naruszeń, Operator wypowiada umowę ze skutkiem natychmiastowym. Kwestie rozliczeń reguluje Regulamin Usług (Bezzwrotność środków).

§ 8. POSTANOWIENIA KOŃCOWE

8.1. Zmiany FUP: Operator zastrzega sobie prawo do zmiany niniejszej Polityki Uczciwego Korzystania z ważnych przyczyn (np. zmiana prawa, nowe zagrożenia bezpieczeństwa, modernizacja infrastruktury). O zmianach Klienci zostaną poinformowani drogą mailową lub

poprzez komunikat w Panelu z wyprzedzeniem co najmniej **30 dni**. Brak sprzeciwu w tym terminie oznacza akceptację zmian. W przypadku sprzeciwu, Klient ma prawo wypowiedzieć umowę ze skutkiem natychmiastowym bez ponoszenia dodatkowych kosztów.

8.2. Integralność: W kwestiach nieuregulowanych w FUP zastosowanie mają zapisy Regulaminu Usług (TOS).