HLG Internet Sp. z o.o.
ul. Długa 5, 39-460 Nowa Dęba, woj. podkarpackie
KRS 0000848385, NIP 8672249951, Regon 386430900
Tel. 15 846 39 99 www.hlgi.pl internet@hlgi.pl

ZLECENIE PRZYDZIELENIA PUBLICZNEGO ADRESU IP W RAMACH USŁUGI DOSTĘPU DO INTERNETU DLA KLIENTÓW INDYWIDUALNYCH

Zleceniodawca:	
Adres instalacji:	
Nr abonenta:	
Data zlecenia:	

Regulamin przydzielania publicznego adresu IPv4 HLG Internet – Nowa Dęba

§1. Postanowienia ogólne

Regulamin określa zasady przydzielania i korzystania z publicznego adresu IPv4 dla Abonentów HLG Internet. Publiczny adres IPv4 udostępniany jest wyłącznie na wniosek Abonenta i stanowi usługę dodatkową do podstawowego pakietu Internetowego.

Przydzielenie adresu IPv4 uzależnione jest od dostępności zasobów adresowych w puli operatora.

Operator przydziela adres losowo z dostępnych zasobów i nie gwarantuje jego niezmienności w trakcie użytkowania. Technicznie jest to przypisanie adresu publicznego do hosta używanego w sieci operatora.

Abonent, zlecając przydzielenie publicznego adresu IP, oświadcza że jest świadomy zagrożeń wynikających z takiej usługi i bierze na siebie pełną odpowiedzialność za zabezpieczenie urządzeń i oprogramowania, podłączonych do sieci domowej.

§2. Warunki uzyskania publicznego adresu IPv4

Abonent musi posiadać aktywną usługę dostępu do Internetu świadczoną przez HLG Internet w ramach grupy taryf dla klientów indywidualnych.

Wniosek o przydzielenie adresu IPv4 można złożyć:

- drogą mailową,
- osobiście w Biurze Obsługi Klienta (BOK),
- poprzez formularz kontaktowy na stronie internetowej Wirtualnego Biura Obsługi Klienta (WBOK).

Przydzielenie adresu wiąże się z miesięczną opłatą abonamentową, zgodnie z obowiązującą ofertą.

Jeden Abonent może otrzymać maksymalnie jeden adres IPv4 na jeden adres instalacji.

§3. Obowiązki Abonenta

Abonent zobowiązany jest do korzystania z adresu IP w sposób zgodny z przepisami prawa oraz Regulaminem Świadczenia Usług Telekomunikacyjnych HLG Internet.

Zabronione jest wykorzystywanie adresu IP do prowadzenia działalności niezgodnej z prawem, wysyłania spamu, ataków sieciowych itp.

W przypadku naruszenia warunków, operator zastrzega sobie prawo do odebrania adresu IPv4 bez zwrotu opłat.

§4. Postanowienia końcowe

Operator zastrzega sobie prawo do zmiany adresu IPv4 przydzielonego Abonentowi w wyjątkowych przypadkach technicznych lub administracyjnych, o czym Abonent zostanie poinformowany z wyprzedzeniem.

W sprawach nieuregulowanych niniejszym Regulaminem mają zastosowanie przepisy Kodeksu cywilnego oraz Prawa Komunikacji Elektronicznej (PKE).

Korzystanie z publicznego adresu IP niesie ze sobą kilka potencjalnych zagrożeń, zwłaszcza jeśli nie jest odpowiednio zabezpieczone środowisko sieciowe. Oto najważniejsze z nich:

🔓 **1. Bezpośrednia dostępność z Internetu**

Publiczny adres IP oznacza, że Twoje urządzenie jest **widoczne i osiągalne z sieci zewnętrznej (Internetu)**. To jak wystawienie drzwi na ulicę – każdy może zapukać, a niektórzy mogą próbować je wyważyć.

🛡️ **2. Większe ryzyko ataków hakerskich**

- **Skanowanie portów:** Cyberprzestępcy regularnie skanują zakresy IP w poszukiwaniu otwartych portów i słabych punktów.
- **Brute-force i exploit attacks:** Jeśli na tym IP działa np. serwer (FTP, SSH, WWW), to może być celem automatycznych ataków próbujących złamać hasła lub wykorzystać podatności.
- **DDoS (Distributed Denial of Service):** Adres IP może zostać zaatakowany przez zalew danych, które mają na celu sparaliżowanie usługi.

🕵️ **3. Ujawnienie lokalizacji i tożsamości**

- Publiczne IP może pozwalać na **przybliżone określenie lokalizacji** użytkownika.
- W przypadku działalności online (np. hosting, fora), IP może być powiązane z konkretną osobą lub firmą.

🧠 **4. Brak ochrony NAT (Network Address Translation)**

- W sieciach z prywatnymi IP użytkownicy są "ukryci" za routerem, który działa jak bufor.
- Publiczny IP oznacza brak tej warstwy ochronnej, więc każde wystawione urządzenie **musi być samodzielnie chronione (firewall, aktualizacje, itp.)**.

📜 **5. Potencjalne problemy prawne**

- Jeśli ktoś wykorzysta Twój adres IP do nielegalnych działań (np. spam, ataki, torrentowanie treści chronionych prawem autorskim), **to Ty możesz zostać pociągnięty do odpowiedzialności**.

✅ **Jak się zabezpieczyć?**

1. **Zainstaluj i skonfiguruj zaporę sieciową (firewall).**
2. **Aktualizuj systemy operacyjne i oprogramowanie.**
3. **Nie wystawiaj niepotrzebnych usług na zewnątrz.**
4. **Stosuj silne hasła i dwuetapowe zabezpieczenia.**
5. **Monitoruj ruch sieciowy.**

.....

Podpis Abonenta