FLEXCLOUD

Polityka dopuszczalnego korzystania i przeciwdziałania nadużyciom FlexCloud

Wersja: 2.0
Data obowiązywania: 28 lipca 2026
Data publikacji: —
Język / Language: PL

SHA-256
fdc5539449d94a7b5bf4bfb1033fe801caf2c02c1a473cafd7051edcd2bc42ae

Spis treści

1. POLITYKA DOPUSZCZALNEGO UŻYTKOWANIA I PRZECIWDZIAŁANIA NADUŻYCIOM (AUP)

2. 1. Cel

AUP chroni Klientów, infrastrukturę i osoby trzecie. Zakazy stosuje się do działań bezpośrednich, zleconych, tolerowanych oraz wykonywanych przez użytkowników, którym Klient udostępnił Usługę.

3. 2. Bezwzględnie zabronione

• phishing, fałszywe panele logowania, podszywanie się pod banki, operatorów, urzędy, sklepy lub osoby;

• malware, ransomware, stealer, keylogger, trojan, botnet, command-and-control;

• wyłudzanie płatności, danych kart, haseł, tokenów, dokumentów lub danych osobowych;

• spam, niezamówione masowe wiadomości, listy pozyskane bez podstawy, spoofing;

• DDoS, DoS, amplification, flood, stress test bez pisemnej zgody właściciela celu;

• nieautoryzowane włamania, skanowanie podatności, brute force i obchodzenie zabezpieczeń;

• przechowywanie lub rozpowszechnianie treści nielegalnych, w tym materiałów seksualnego wykorzystywania dzieci;

• handel skradzionymi kontami, danymi, kartami, tożsamościami, licencjami lub dostępami;

• naruszenia własności intelektualnej na skalę świadomą lub powtarzalną;

• usługi służące ukrywaniu bezprawnej działalności, jeżeli Klient wie o takim celu;

• działania zagrażające stabilności sieci, adresacji IP lub reputacji FlexCloud.

4. 3. Zastosowania warunkowe

Publiczne proxy, VPN, Tor exit, masowe scrapowanie, crawling, mining, serwery pocztowe, skanery, testy bezpieczeństwa i automaty wysokiego obciążenia wymagają wyraźnego dopuszczenia w planie lub wcześniejszej zgody FlexCloud.

5. 4. Reagowanie

1. FlexCloud może ograniczyć port, adres IP, proces, domenę, plik lub całą Usługę.

2. Środek powinien być możliwie ukierunkowany, chyba że zagrożenie wymaga odizolowania całej Usługi.

3. Przy aktywnym phishingu, malware, botnecie lub ataku działanie może być natychmiastowe.

4. Klient może złożyć wyjaśnienia i odwołanie. FlexCloud nie ma obowiązku przywrócenia treści oczywiście bezprawnej ani konfiguracji nadal zagrażającej bezpieczeństwu.

6. 5. Współpraca Klienta

Klient ma obowiązek w rozsądnym terminie usunąć naruszenie, zabezpieczyć system, zmienić dane dostępowe, zaktualizować oprogramowanie i przekazać wymagane wyjaśnienia.

7. 6. Nadużycia płatnicze

Zakazane jest używanie cudzej metody płatności, zakładanie kont na fikcyjne dane, obchodzenie blokad, kupowanie Usług dla osób wcześniej zablokowanych oraz wykorzystywanie sandboxu jako dowodu realnej zapłaty.