Acceptable Use Policy

Verze dokumentu: 2026-07-25
Kategorie: smluvni

Provozovatel: Kibios s.r.o., IČO 29814995, se sídlem Brněnská 305/32, 664 44 Ořechov.
Kontakt: info@kibios.com
Online verze: https://kibios.com/pravni/acceptable-use-policy

1. Úvod

Tato Acceptable Use Policy (AUP) stanoví pravidla přijatelného používání služeb Kibios s.r.o. (dále jen „Kibios“ nebo „poskytovatel“) klientem (dále jen „klient“) a jeho uživateli. AUP je součástí smluvního rámce Kibios (MSA, VOP, SLA, DPA, SOW) a uplatní se na všechny služby Kibios, včetně free testů, demo a pilotních projektů.

2. Rozsah působnosti AUP

2.1. AUP se vztahuje na:

- všechny služby poskytované Kibios (monitoring, správa systémů, hosting, zálohy, pen-testy, IVR/voicemail atd.),
- všechny systémy a prostředky, které Kibios klientovi poskytuje nebo spravuje,
- všechny uživatele, kteří služby Kibios využívají jménem klienta.

2.2. Klient odpovídá za to, že jeho zaměstnanci, dodavatelé a další osoby používající služby Kibios jsou s AUP seznámeni a dodržují ji.

3. Obecné zásady

3.1. Služby Kibios lze používat pouze:

- v souladu s právními předpisy,
- v souladu s MSA, VOP, SLA, DPA a touto AUP,
- k účelům, které nejsou nezákonné, neetické ani škodlivé vůči třetím osobám.

3.2. Klient nesmí služby Kibios používat způsobem, který:

- ohrožuje bezpečnost nebo stabilitu infrastruktury Kibios nebo třetích stran,
- porušuje práva třetích osob (např. autorská práva, osobnostní práva),
- je v rozporu se zásadami kybernetické bezpečnosti nebo dobrými mravy.

4. Zakázané činnosti (misuse / abuse)

Bez výslovného a písemného souhlasu poskytovatele (např. v rámci pen-testu s RoE) klient nesmí prostřednictvím služeb Kibios:

4.1. Šíření škodlivého kódu

- šířit, hostovat nebo provozovat malware (viry, trojské koně, ransomware, spyware, keyloggery, botnet klienty apod.),

- provozovat command-and-control (C2) servery nebo jiné infrastruktury pro botnety,
- záměrně rozesílat soubory nebo odkazy obsahující škodlivý kód.

4.2. Útoky na systémy

- provádět DDoS/DoS útoky, port scanning, brute-force útoky, exploitování zranitelností bez oprávnění vlastníka,
- provádět penetrační testy nebo hacking na systémy třetích stran bez jejich souhlasu,
- využívat infrastrukturu Kibios k neoprávněnému přístupu k počítačovým systémům.

4.3. Spam, phishing a podvodné jednání

- rozesílat nevyžádanou hromadnou poštu (spam),
- provozovat phishingové kampaně, falešné login stránky, podvodné weby nebo sociální inženýrství,
- imitovat identity třetích osob nebo se vydávat za jiný subjekt bez souhlasu.

4.4. Nelegální obsah

- hostovat, ukládat nebo distribuovat obsah, který je nezákonný (např. dětská pornografie, obsah podporující terorismus, podněcování nenávisti, nelegální warez, pirátský software),
- porušovat autorská práva, databázová práva, ochranné známky nebo jiné duševní vlastnictví třetích osob.

4.5. Cryptomining a zneužití zdrojů

- provozovat cryptomining (těžbu kryptoměn) na infrastruktuře Kibios nebo spravovaných systémech klienta bez výslovného ujednání,
- zneužívat zdroje (CPU, RAM, bandwidth, storage) k jiným účelům, než které jsou sjednány ve Smlouvě/SOW.

4.6. Obcházení bezpečnostních opatření

- obcházet, vypínat nebo narušovat bezpečnostní opatření Kibios nebo třetích stran (firewally, IDS/IPS, antiviry, přístupové kontroly),
- pokoušet se získat neoprávněný přístup k administrátorským účtům Kibios.

5. Speciální režim – penetrační testy a bezpečnostní testování

5.1. Pokud služby Kibios zahrnují penetrační testy nebo aktivní bezpečnostní testování:

- veškeré testy musí být předem dohodnuty v Rules of Engagement (RoE),
- testy se provádějí pouze na systémech, které jsou in-scope (ve vlastnictví nebo pod kontrolou klienta / oprávněného subjektu),
- zakázané útoky (např. DoS, destruktivní payload) se neprovádějí, ledaže jsou výslovně povolené v RoE.

5.2. AUP se v těchto případech uplatní tak, že výše uvedené zakázané činnosti jsou povoleny pouze v rozsahu a způsobem uvedeným v RoE, který klient elektronicky odsouhlasí.

6. Povinnosti klienta

6.1. Klient je povinen:

- používat služby Kibios pouze k účelům uvedeným ve Smlouvě/SOW,

- zabránit svým uživatelům v porušování AUP,
- zajistit, aby přístupové údaje (účty, hesla, tokeny) nebyly sdíleny neoprávněně,
- neprodleně informovat Kibios o jakémkoli podezření na zneužití služeb, účtů nebo infrastruktury.

6.2. Klient odpovídá za činnost osob, kterým umožní přístup k službám Kibios (zaměstnanci, dodavatelé, partneři), jako za svou vlastní.

7. Abuse process (řešení stížností a incidentů)

7.1. Pokud se Kibios dozví o možném porušení AUP (např. stížnost třetí osoby, bezpečnostní incident, oznámení CERT/NÚKIB):

- prověří základní fakta, logy a technické souvislosti,
- může klienta kontaktovat s žádostí o vysvětlení nebo nápravu.

7.2. Kibios informuje klienta o zjištěném possible abuse. Klient je povinen:

- reagovat bez zbytečného odkladu, obvykle do 24 hodin od oznámení,
- přijmout přiměřená nápravná opatření (zastavení kampaně, odstranění nelegálního obsahu, reset účtů, zvýšení zabezpečení).

7.3. Pokud klient nereaguje nebo nápravu neprovede:

- Kibios je oprávněn dočasně pozastavit poskytování konkrétní služby,
- v krajním případě i zcela přerušit poskytování služeb, pokud je to nezbytné k ochraně třetích osob, infrastruktury Kibios nebo plnění právních povinností.

7.4. Kibios může v případě závažného porušení AUP (např. trestná činnost, velký bezpečnostní incident) spolupracovat s příslušnými orgány (OČTK, NÚKIB, CERT) a poskytnout jim nezbytné informace v rozsahu dovoleném právem.

8. Důsledky porušení AUP

8.1. Porušení AUP může vést k:

- pozastavení nebo omezení služeb,
- okamžitému ukončení části nebo všech služeb podle MSA/VOP,
- nárokům Kibios na náhradu škody, pokud porušení AUP vedlo ke škodě nebo incidentu,
- oznámení relevantním orgánům v případě podezření na trestný čin nebo závažné porušení právních předpisů.

8.2. Klient bere na vědomí, že porušení AUP může být považováno za podstatné porušení smlouvy ve smyslu § 2002 OZ a vést k odstoupení od Smlouvy.

9. Free testy, demo a self-service

9.1. AUP platí i pro:

- free bezpečnostní testy,
- demo prostředí,

- pilotní projekty,
- self-service nástroje na webu Kibios.

9.2. Klient (nebo osoba jednající za klienta) v těchto režimech nesmí:

- testovat nebo skenovat systémy třetích stran bez jejich souhlasu,
- provádět testy, které by mohly vést k poškození infrastruktury,
- využívat free nástroje k hromadnému nebo automatizovanému zneužití.

10. Elektronická akceptace AUP

10.1. Klient bere na vědomí, že AUP je přijímána elektronicky, zejména:

- zaškrtnutím souhlasu při registraci, objednávce nebo v klientském portálu,
- potvrzením „Souhlasím s Acceptable Use Policy (AUP) Kibios“ v dashboardu.

10.2. Za odsouhlasenou se AUP považuje okamžikem, kdy oprávněná osoba klienta:

- potvrdí, že se seznámila s AUP,
- zaškrtne příslušné pole (checkbox) a
- odešle formulář (tlačítko „Souhlasím / Potvrdit“).

10.3. Kibios uchovává log elektronické akceptace (čas, účet, IP, verze AUP) jako důkaz o souhlasu klienta.

11. Změny AUP

11.1. Kibios může AUP aktualizovat, zejména v důsledku:

- změn právních předpisů,
- změn technologií, rizik nebo typických forem zneužití,
- rozšíření nebo omezení služeb Kibios.

11.2. O podstatných změnách AUP, které se dotýkají klienta, bude klient informován (e-mail, klientský portál) před účinností nové verze.

11.3. Pokud klient nesouhlasí s aktualizací AUP, může ukončit služby podle MSA/VOP ke dni účinnosti nové AUP.